

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2002-358283

(43)Date of publication of application : 13.12.2002

(51)Int.Cl. G06F 15/00

H04L 9/32

(21)Application number : 2001-166114 (71)Applicant : NEC CORP

(22)Date of filing : 01.06.2001 (72)Inventor : TANAKA HIROYUKI

(54) USER AUTHENTICATION COLLABORATION METHOD, SYSTEM AND PROGRAM

(57)Abstract:

PROBLEM TO BE SOLVED: To provide a user authentication collaboration system and a method therefor that permit the collaboration of authentication even on a WWW server unable to use a server for performing the authentication.

SOLUTION: The WWW server 2 has means 21, 22 that, if a terminal 1 transmits a request from a user and user information for performing user authentication, receive them and transmit the user information to an authentication server 4, an authentication information generating means 23 that, if the authentication in the authentication server is proved successful, generates authentication information from the user information on the user and time information, and a means 21 that transmits the generated authentication information together with the request result to the terminal. The terminal 1, in transmitting a request to the WWW server 3, transmits the authentication information. The WWW server 3 has an authentication collaborative processing means 34 that extracts the user information and the time information from the authentication information and performs the collaborative processing of authentication, and a means 31 that, if the correctness of the authentication information is verified and the user is authenticated, accepts the user's request and transmits the request result together with the newly generated authentication information to the terminal.

LEGAL STATUS

[Date of request for examination] 28.05.2002
[Date of sending the examiner's decision of rejection] 31.10.2006
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]
[Date of final disposal for application]
[Patent number]
[Date of registration]
[Number of appeal against examiner's decision of rejection]
[Date of requesting appeal against examiner's decision of rejection]
[Date of extinction of right]

CLAIMS

[Claim(s)]

[Claim 1] The step to which the information offer server of 1 accessed through a network from a terminal generates authentication information for the user information transmitted from said terminal from reception, and said user information and hour entry, The step at which said information offer server of 1 transmits said generated authentication information to said terminal, It is the information offer server accessed through a network from said terminal. The user authentication cooperation approach characterized by what the information offer server which performs cooperation processing of authentication takes out user information and a hour entry for said authentication information transmitted from said terminal from reception and said authentication information, and contains the step which performs an authentication judging for.

[Claim 2] Said information offer server of 1 said user information transmitted to said information offer server of 1 from said terminal In said information offer server of 1 which received the authentication result in said authentication server when the step transmitted to the authentication server linked to said information offer server of 1 was performed and authentication was correctly performed by said authentication server The user authentication cooperation approach according to claim 1 characterized by what the step which generates said authentication information, the step which transmits said authentication information to said terminal, and ** are performed for.

[Claim 3] The user-authentication cooperation approach according to claim 1 which carries out as the description in what said user information is taken out from said authentication information, and the step which transmits said authentication information which newly generated authentication information and was newly generated by said terminal from said user information and hour entry is included for in said information offer server which performs cooperation processing of authentication when authentication is successful at the step which performs said authentication judging.

[Claim 4] The step which transmits said authentication information to said information offer server which performs cooperation processing of authentication when said terminal which received said newly generated authentication information transmits a demand to the information offer server which performs cooperation processing of authentication, In said information offer server which performs cooperation processing of authentication User information and a hour entry are taken out for said authentication information transmitted from said terminal from reception and said authentication information. Said user information taken out from said authentication information when an authentication judging was performed and authentication was successful, The user authentication cooperation approach according to claim 3 characterized by what the step which transmits said authentication information which newly generated authentication information and was newly generated by said terminal from the hour entry is included for.

[Claim 5] The user authentication cooperation approach according to claim 1 to 4 characterized by what said hour entry used for generation of said authentication information is a hour entry of the system clock of the information offer server which generates said authentication information.

[Claim 6] A terminal in the demand from a user, the step which transmits the user information for performing user authentication to the information offer server of 1, and said information offer server of 1 The step which generates authentication information in the authentication information generation section of said information offer server of 1 when said user information is transmitted to the authentication server which said information offer server of 1 connects and authentication by said authentication server is successful, Said information offer server of 1 said authentication information generated in said authentication information generation section of said information offer server of 1 with a demand result When transmitting a demand to the step transmitted to said terminal, and other information offer servers to which said terminal cooperates with said information offer server of 1, and performs cooperation processing of authentication, with said demand By the step which transmits an information offer server besides the above, and an information offer server besides the above, said authentication information Said authentication information transmitted from said terminal in reception and the authentication cooperation processing section In the step which performs cooperation processing of

authentication based on said received authentication information, and an information offer server besides the above The user authentication cooperation approach characterized by what a demand of said user is received and it has for the step which transmits the authentication information newly generated with the demand result to said terminal when the rightness of authentication information is verified and said user is attested by cooperation processing of said authentication.

[Claim 7] The user authentication cooperation approach according to claim 6 that authentication information generated in said authentication information generation section is characterized by what such information is enciphered for including user information, a hour entry, and check data.

[Claim 8] The step to which the step which performs cooperation processing of authentication in said authentication cooperation processing section decodes said received authentication information, The step which takes out user information and a hour entry from said decoded authentication information when the step which inspects the check data of said decoded authentication information, and inspection of said check data are successful, The user authentication cooperation approach according to claim 6 or 7 characterized by what the step which inspects time amount based on said taken-out hour entry, and the step considered as an authentication success when said time amount inspection is successful are included for.

[Claim 9] The user authentication cooperation approach according to claim 6 or 7 characterized by what user authentication processing using said authentication server is performed in access to the first information offer server, and authentication cooperation processing by the information offer server is performed for to the demand from a user by access to the continuing information offer server.

[Claim 10] It has the authentication cooperation processing section in which said information offer server of 1 performs authentication cooperation of authentication. In said information offer server of 1 The step which requests generation of authentication information from the authentication information generation section of said information offer server of 1 when cooperation processing of authentication of the authentication information transmitted from said terminal in reception and said authentication cooperation processing section is performed and an authentication judging is successful, Said authentication information generation section of said information offer server of 1 The user authentication cooperation approach according to claim 6 characterized by what the step which generates authentication information for the user information which said authentication cooperation processing section of said information offer server of 1 acquired from said authentication information from reception, and said user information and hour entry is included for.

[Claim 11] The information offer server besides the above which performs cooperation processing of authentication has the authentication information generation section. said -- others -- the case where performed cooperation processing of authentication in the authentication cooperation processing section of

an information offer server, and an authentication judging is successful -- said -- others -- with the step which requests generation of authentication information from the authentication information generation section of an information offer server The authentication information generation section of an information offer server besides the above The step which generates authentication information for the user information which said authentication cooperation processing section acquired from said authentication information from reception, and said user information and hour entry, The user authentication cooperation approach according to claim 6 or 10 characterized by what an information offer server besides the above contains a user's demand result and the step which transmits said generated authentication information to said terminal for.

[Claim 12] The user information for which the information offer server of 1 accessed through a network from a terminal was inputted from said terminal, and was transmitted to said information offer server of 1, From the hour entry in said information offer server of 1, generate authentication information and said generated authentication information It is the information offer server which is equipped with a means to transmit to said terminal, and is accessed through a network from said terminal. The user authentication cooperation system characterized by what the information offer server which performs cooperation processing of authentication decoded reception and said authentication information for said authentication information transmitted from said terminal, user information and a hour entry were taken out, and it has a means to perform an authentication judging for.

[Claim 13] It has a terminal and two or more information offer servers accessed through a network from this terminal. To said two or more information offer servers At least one information offer server connected to an authentication server, and at least one information offer server which performs cooperation processing of authentication, The information offer server of 1 connected to **** rareness and said authentication server A means to receive this and to transmit said user information to said authentication server when said terminal transmits the demand from a user, and the user information for performing user authentication to said information offer server of 1, When authentication by said authentication server is successful, an authentication information generation means to generate authentication information from said user information and hour entry, and said generated authentication information with a demand result It has a means to transmit to said terminal. Said terminal When transmitting a demand to said information offer server which performs cooperation processing of authentication, said authentication information transmitted from said information offer server of 1 Said information offer server which is equipped with a means to transmit to said information offer server which performs cooperation processing of authentication, and performs cooperation processing of authentication By authentication cooperation processing means to take out user information and a hour entry and to perform cooperation processing of authentication from said

authentication information, and cooperation processing of said authentication It is the user authentication cooperation system characterized by what the demand of said user was received and it has a means to transmit the authentication information newly generated with the demand result to said terminal for when the rightness of authentication information is verified and said user is attested.

[Claim 14] The user authentication cooperation system according to claim 13 characterized by what what enciphered the information which said authentication information generation means of said information offer server of 1 becomes from said user information, a hour entry, and check data is outputted for as said authentication information.

[Claim 15] The user authentication cooperation system according to claim 13 which performs user authentication processing using said authentication server in access to the first information offer server, and is characterized by performing authentication cooperation processing of an information offer server to the demand from a user by continuing access.

[Claim 16] A user demand processing means by which said information offer server of 1 processes a demand of the user from said terminal, When an authentication demand is performed to said authentication server and authentication is successful by said authentication server, it has an authentication demand means to require that authentication information should be generated. Said authentication information generation means In response to the demand from said authentication demand means, it is the user authentication cooperation system according to claim 13 which generates said authentication information from said user information and hour entry, and is characterized by what said user demand processing means transmits a demand result and said generated authentication information for to said terminal.

[Claim 17] Said information offer server which performs cooperation processing of authentication is equipped with a user demand processing means to process a demand of the user from said terminal. Said authentication cooperation processing means performs cooperation processing of authentication for the authentication information transmitted with a demand from said terminal based on reception and said authentication information. By authentication cooperation processing with said authentication cooperation processing means The user authentication cooperation system according to claim 13 characterized by what a demand of said user is received and said authentication information newly generated with the demand result is transmitted for to said terminal with said user demand processing means when the rightness of authentication information is verified and said user is attested.

[Claim 18] The user authentication cooperation system according to claim 13 by which the inspection result of said hour entry is characterized a right case by what considers as an authentication success including a means to by which said authentication cooperation processing means decodes said authentication information, a means inspect the check data of said decoded authentication information, a means

to by which the inspection result of said check data takes out user information and a hour entry from said decoded authentication information a right case, and a means conduct inspection of said hour entry.

[Claim 19] Said information offer server of 1 is further equipped with an authentication cooperation processing means. Said information offer server of 1 Said authentication cooperation processing means of reception and said information offer server of 1 performs authentication cooperation for the authentication information transmitted from said terminal. When an authentication judging is successful, generation of authentication information is requested to said authentication information generation means of said information offer server of 1. Said authentication information generation means of said information offer server of 1 The user authentication cooperation system according to claim 13 characterized by what authentication information is generated [a thing] for the user information which said authentication cooperation processing means acquired from said authentication information from reception, said user information, and a hour entry.

[Claim 20] Said information offer server which performs cooperation processing of authentication is equipped with an authentication information generation means. Said information offer server which performs cooperation processing of authentication performs authentication cooperation with said authentication cooperation processing means. When an authentication judging is successful, generation of authentication information is requested from said authentication information generation means of said information offer server which performs cooperation processing of authentication. Said authentication information generation means of said information offer server which performs cooperation processing of authentication The user authentication cooperation system according to claim 13 or 19 characterized by what authentication information is generated for the user information which said authentication cooperation processing means acquired from said authentication information from reception, user information, and a hour entry, and a user's demand result and said authentication information are transmitted for to said terminal.

[Claim 21] The information offer server of 1 accessed through a network from a terminal The demand from [from the (a) aforementioned terminal] a user, The processing which receives the user information for performing user authentication, and transmits said user information to said authentication server, (b) When authentication by said authentication server is successful, the authentication information by which the (c) aforementioned generation was carried out with the authentication information generation processing which generates authentication information from said user information and hour entry with a demand result The information offer server which has the processing transmitted to said terminal, is accessed through a network from a terminal, and performs cooperation processing of said information offer server of 1 and authentication (d) by authentication cooperation processing in which take out user information and a hour entry and cooperation

processing of authentication is performed from said authentication information transmitted from said terminal; and the (e) aforementioned authentication cooperation processing It is a program for performing said each processing by said each information offer server including the processing which transmits the authentication information which received the demand of said user and was newly generated with the demand result when the rightness of authentication information was verified and said user was attested to said terminal.

[Claim 22] The program for performing processing which generates authentication information and enciphers this authentication information further from said user information, hour entry, and check data by said authentication information generation processing in a program according to claim 21 by said information offer server.

[Claim 23] The program for performing said the processing of each by said information offer server in a program according to claim 21 including the processing whose the authentication cooperation processing of said decodes said authentication information, the processing which inspect the check data of said decoded authentication information, the processing to which said authentication information to the user information that the inspection result of said check data was decoded the right case, and a hour entry take out, and the processing carry out inspection of said hour entry.

[Claim 24] A means by which the information offer server accessed through a network from a terminal receives the user information for performing user authentication transmitted from said terminal, and transmits said user information to said authentication server, Information offer server equipment characterized by what it has an authentication information generation means to generate authentication information from said user information and hour entry, and a means to transmit said generated authentication information to said terminal for when authentication by said authentication server is successful.

[Claim 25] Information offer server equipment equipped with a means to receive the user information which network connection is carried out to a terminal and transmitted from said terminal, to generate authentication information from said user information and hour entry, and to transmit said generated authentication information to said terminal, By authentication cooperation processing means to take out user information and a hour entry and to perform cooperation processing of authentication from said authentication information which is the information offer server which performs cooperation processing of authentication, and was transmitted from said terminal, and cooperation processing of said authentication It is information offer server equipment characterized by what the demand of said user was received and it has a means to transmit the authentication information newly generated with the demand result to said terminal for when the rightness of authentication information is verified and said user is attested.

[Claim 26] The information offer server equipment according to claim 24 with which the inspection result of said hour entry is characterized a right case by what

considers as an authentication success including a means to by which said authentication cooperation processing means decodes said authentication information, a means inspect the check data of said decoded authentication information, a means to by which the inspection result of said check data takes out user information and a hour entry from said decoded authentication information a right case, and a means conduct inspection of said hour entry.

DETAILED DESCRIPTION

[Detailed Description of the Invention]

[0001]

[Field of the Invention] Especially this invention relates to a program about an authentication system and an approach at the approach, system, and equipment list which perform authentication cooperation processing by the server.

[0002]

[Description of the Prior Art] As a user authentication cooperation system, in the network system equipped with two or more WWW (World Wide Web) servers, once a user attests, the WWW [access / be / possible] server cooperation system covering two or more pages or a different WWW server based on invisible ID of the given meaning is proposed by JP,11-31129,A in the authentication effective time. In this WWW server cooperation system, the host who processes cooperation using Session ID When a HTML (HyperText Markup Language) document is analyzed from the browser notified from one of two or more WWW servers and Session ID is not given The input request of User Information is transmitted to a browser through a WWW server. Generate the session ID of a meaning to the demand to which transmitted User Information was analyzed and registration was permitted, and again, while transmitting the HTML document which embedded Session ID through the WWW server to a browser Effective-time information is managed and authentication is permitted at the time of effective-time information within the limits. That is, when authentication is required, ID and the password which were transmitted with the terminal are transmitted to a host via a WWW server, and authentication is performed. When authentication is successful with a host, Session ID is generated by the host, the session ID is sent to a terminal via a WWW server with a result, at the time of access from a user, Session ID is automatically added to the demand transmitted from a terminal, and the session ID is verified by the host.

[0003] However, this user authentication cooperation system has the following troubles.

[0004] The WWW server for which a host cannot use the 1st trouble is impossible

[cooperation]. The reason is because verification of Session ID and generation are chiefly performed by the host.

[0005] The 2nd trouble is that the response falls, when the demand from a user grows. The reason is because all WWW servers are considered as the configuration which requires verification and generation of Session ID to the same host for every access from all users.

[0006] moreover, in JP,2000-222360,A It has a client means, an authentication server means, and a license server means. A client means Confidential information is shared with an authentication server. An authentication server means An authentication ticket including the collating information which performed the irreversible operation f for confidential information n times is published, and a client means shows the presentation information which performed the irreversible operation f to the license server n-k times. A license server Whether a line's being in agreement with collating information k times in the irreversible operation f at presentation information, and the authentication system and approach of checking are proposed. At the WWW server and terminal which cannot connect this system to an authentication server means and a license server means, either, it is inapplicable. Moreover, the substitute server which has the authentication response Management Department is prepared between a client and two or more servers, and the authentication response approach and equipment which execute the response of the authentication information over two or more servers by proxy about the client which the authentication response Management Department attested the client and once attested are indicated by JP,10-177552,A, for example.

[0007]

[Problem(s) to be Solved by the Invention] Therefore, the technical problem which this invention tends to solve is for the WWW server which cannot use the server which attests to also provide with a program the approach and system which enable cooperation of authentication, and an equipment list.

[0008]

[Means for Solving the Problem] The approach concerning this invention which offers said The means for solving a technical problem The user information for which the information offer server of 1 accessed through a network from a terminal was inputted from said terminal, and was transmitted to said information offer server of 1, The step which generates authentication information and transmits said generated authentication information to said terminal from the hour entry in said information offer server of 1, In the information offer server which is an information offer server accessed through a network from said terminal, and performs cooperation processing of authentication Reception and said authentication information are decoded for said authentication information transmitted from said terminal, user information and a hour entry are taken out, and the step which performs an authentication judging is included.

[0009] A terminal the approach concerning this invention by the demand from a user,

the step which transmits the user information for performing user authentication to the information offer server of 1, and said information offer server of 1 The step which generates authentication information in the authentication information generation section of said information offer server of 1 when said user information is transmitted to an authentication server and authentication by said authentication server is successful, Said information offer server of 1 said authentication information generated in said authentication information generation section of said information offer server of 1 with a demand result The step which transmits an information offer server besides the above for said authentication information when transmitting a demand to the step transmitted to said terminal, and other information offer servers to which said terminal cooperates with said information offer server of 1, and performs cooperation processing of authentication, In an information offer server besides the above, said authentication information transmitted from said terminal in reception and the authentication cooperation processing section In the step which performs cooperation processing of authentication based on said authentication information, and an information offer server besides the above When the rightness of authentication information is verified and said user is attested by cooperation processing of said authentication, a demand of said user is received and it has the step which transmits the authentication information newly generated with the demand result to said terminal.

[0010] In another aspect, the system concerning this invention The user information for which the information offer server of 1 accessed through a network from a terminal was inputted from said terminal, and was transmitted to said information offer server of 1, From the hour entry in said information offer server of 1, generate authentication information and said generated authentication information It is the information offer server which is equipped with a means to transmit to said terminal, and is accessed through a network from said terminal. The information offer server which performs cooperation processing of authentication decoded reception and said authentication information for said authentication information transmitted from said terminal, took out user information and a hour entry, and is equipped with a means to perform an authentication judging.

[0011] Furthermore, the program which relates to this invention in another aspect The information offer server of 1 accessed through a network from a terminal The demand from [from the (a) aforementioned terminal] a user, The processing which receives the user information for performing user authentication, and transmits said user information to said authentication server, (b) When authentication by said authentication server is successful, the authentication information by which the (c) aforementioned generation was carried out with the authentication information generation processing which generates authentication information from said user information and hour entry with a demand result The information offer server which has the processing transmitted to said terminal, is accessed through a network from a

terminal, and performs cooperation processing of said information offer server of 1 and authentication (d) by authentication cooperation processing in which take out user information and a hour entry and cooperation processing of authentication is performed from said authentication information transmitted from said terminal, and the (e) aforementioned authentication cooperation processing When the rightness of authentication information is verified and said user is attested, a demand of said user is received and it consists of a program for performing said each processing by said each information offer server including the processing which transmits the authentication information newly generated with the demand result to said terminal.

[0012]

[Embodiment of the Invention] The gestalt of operation of this invention is explained. This invention in the gestalt of desirable 1 operation, from the terminal (1 of drawing 1) which has browser ability The information offer server (WWW (World Wide Web) server) (2 of drawing 1) accessed through networks, such as IP (Internet Protocol) network A means to receive the user information which was inputted from the terminal (1 of drawing 1) and was transmitted to the WWW server (2) (21 of drawing 1). It has a means (23 of drawing 1) to generate authentication information, and a means (21 of drawing 1) to transmit said generated authentication information to said terminal, from user information and the hour entry in said WWW server of 1. Moreover, it was accessed through the network from the terminal (1 of drawing 1), and the WWW server (3 of drawing 1) which performs cooperation processing of authentication is equipped with a means (31 of drawing 1) to receive the authentication information transmitted from the terminal (1 of drawing 1), and a means (34 of drawing 1) to perform an authentication judging by decoding this authentication information, taking out user information and a hour entry, and conducting time amount inspection.

[0013] This invention the WWW server (2 of drawing 1) of 1 connected to an authentication server (4 of drawing 1) in the gestalt of desirable 1 operation A terminal (1 of drawing 1) the demand from a user, and the user information for performing user authentication A means to receive this and to transmit said user information to an authentication server (4 of drawing 1) when it transmits to a WWW server (2 of drawing 1) (21 of drawing 1, 22). When authentication by the authentication server (4 of drawing 1) is successful, it has an authentication information generation means (23 of drawing 1) to generate authentication information from said user information and hour entry of said user, and a means (21 of drawing 1) to transmit said generated authentication information to said terminal with a demand result.

[0014] The terminal (1 of drawing 1) is equipped with a means (11 of drawing 1) to transmit said authentication information transmitted from the WWW server (2 of drawing 1) to said WWW server (3 of drawing 1) which performs cooperation processing of authentication when transmitting a demand to the WWW server (3 of

drawing 1) which performs cooperation processing of authentication.

[0015] The WWW server (3 of drawing 1) which performs cooperation processing of authentication By authentication cooperation processing means (34 of drawing 1) to take out user information and a hour entry and to perform cooperation processing of authentication from said authentication information, and cooperation processing of said authentication When the rightness of authentication information is verified and said user is attested, the demand of said user was received and it has a means (31 of drawing 1) to transmit the authentication information newly generated with the demand result to said terminal.

[0016] As for this invention, such information is enciphered for the authentication information generated by said WWW server of 1 in the gestalt of desirable 1 operation including user information, a hour entry, and check data.

[0017] In the WWW server (3 of drawing 1) which performs cooperation processing of authentication an authentication cooperation processing means (34 of drawing 1) A means (B1 of drawing 4) to decode authentication information, and a means to inspect the check data of the decoded authentication information (B-2 of drawing 4), The inspection result of said hour entry considers as an authentication success a right case including the means (B3 of drawing 4) which takes out authentication information to the user information by which the inspection result of these check data was decoded the right case, and a hour entry, and a means (B4 of drawing 4) to conduct inspection of said hour entry.

[0018] In the gestalt of another operation of this invention, the WWW server (5 of drawing 5) equipped with the above-mentioned authentication information generation means (23 of drawing 5) is good also as a configuration further equipped with the authentication cooperation processing means (54 of drawing 5). A WWW server (5 of drawing 5) the authentication information transmitted from the terminal (1 of drawing 5) Reception, When the authentication cooperation processing means (54 of drawing 5) performed authentication cooperation and an authentication judging is successful, Requesting generation of authentication information to an authentication information generation means (54 of drawing 5), an authentication information generation means (23 of drawing 5) generates authentication information for the user information which the authentication cooperation processing means (54 of drawing 5) acquired from said authentication information from reception, user information, and a hour entry.

[0019] The WWW server (6 of drawing 5) which performs cooperation processing of authentication is good also as a configuration further equipped with the authentication information generation means (63 of drawing 5). Said WWW server (6 of drawing 5) which performs cooperation processing of authentication performs authentication cooperation with said authentication cooperation processing means (34 of drawing 5). When an authentication judging is successful, generation of authentication information is requested from said authentication information generation means (63 of drawing 5) of the WWW server (6 of drawing 5) which performs cooperation processing of

authentication. Said authentication information generation means (63 of drawing 5) generates authentication information for the user information which said authentication cooperation processing means (34 of drawing 5) acquired from said authentication information from reception, user information, and a hour entry, and a user's demand result and authentication information are transmitted to said terminal. [0020] The processing and a function are realized by the program by which the authentication information generation means in a WWW server and an authentication cooperation processing means are performed with the node computer of a WWW server.

[0021] It can be made to perform cooperation of authentication of a user, without a WWW server using an authentication processing server, in being the environment which an authentication processing server cannot use in common when two or more WWW servers attest a user.

[0022] Drawing 1 is drawing showing the system configuration of the gestalt of 1 operation of this invention. In drawing 1 , a terminal (1) is connected to a WWW server (2) etc. through networks, such as an Internet Protocol network, and an authentication server (4) is provided with the user information for authentication that it was inputted from the terminal (1) through a WWW server (2).

[0023] The user demand transceiver means (11) of a terminal (1) transmits the demand from a user to the user demand processing means (21) of a WWW server (2). At the time of the first time, both user information, such as the user ID for performing user authentication and a password, is transmitted to the demand transmitted.

[0024] The user demand processing means (21) of a WWW server (2) transmits user information to an authentication demand means (22). An authentication demand means (22) transmits the user information to the authentication processing means (41) of an authentication server (4), and waits for a result with the available user.

[0025] When authentication is successful with the authentication processing means (41) of an authentication server (4), the result of an authentication success is returned to the authentication demand means (22) of a WWW server (2), and an authentication demand means (22) requests generation of authentication information from an authentication information generation means (23).

[0026] The user demand processing means (21) of a WWW server (2) transmits the authentication information generated by the authentication information generation means (23) to the user demand transceiver means (11) of a terminal (1) with the demand result. User information and a hour entry are included, and when transmitting the demand which a user follows, a user demand transceiver means (11) transmits to this authentication information automatically [both].

[0027] Then, when a user transmits a demand to the user demand processing means (31) of the 2nd WWW server (3) which cooperates with a WWW server (2), authentication information is both transmitted.

[0028] In that case, authentication cooperation processing is performed by the

authentication cooperation processing means (34) of a WWW server (3) based on the authentication information.

[0029] Although a demand of the user will be received when the rightness of authentication information is verified and a user is attested by authentication cooperation processing, the user demand processing means (31) of a WWW server (3) transmits the demand result to the user demand transceiver means (11) of a terminal (1).

[0030] Thereby, it makes it possible to perform user cooperation, without using an authentication processing server.

[0031]

[Example] The example of this invention is explained that it should explain to still more concrete about the above-mentioned gestalt of operation, and a detail. Drawing 1 is drawing showing an example of the system configuration of one example of this invention. When drawing 1 is referred to, the system concerning one example of this invention contains the terminal 1 with which a user transmits and receives a demand, the WWW server 2 which processes the user demand, the 2nd WWW server 3 which cooperates with the WWW server 2 and processes the user demand, and the authentication server 4 which processes a user's authentication information. In addition, in this example, although the contents of the information which a WWW server offers, and a class are not asked, a user's authentication shall be needed in activation of a processing demand.

[0032] A terminal 1 transmits a demand of a user to a WWW server, and is equipped with a user demand transceiver means 11 to receive the processing result from a WWW server. The user demand transceiver means 11 is automatically transmitted with this demand, when there is authentication information which the authentication information generation means 23 of the WWW server 2 generated, in case a demand is transmitted. When a demand is processed, the demand result transmitted from the user demand processing means 21 of the WWW server 2 and the user demand processing means 31 of the WWW server 3 is received.

[0033] The WWW server 2 is equipped with the user demand processing means 21, the authentication demand means 22, and the authentication information generation means 23.

[0034] In the WWW server 2, the user demand processing means 21 processes the demand sent from the user demand transceiver means 11. Delivery and an authentication result are obtained for the user ID transmitted to the first time demand with the demand, and user information like a password for the authentication demand means 22. In case authentication by the authentication server 2 is successful and the WWW server 2 transmits a demand result to a terminal 1, the authentication information generated with the authentication information generation means 23 is transmitted to the user demand transceiver means 11 of a terminal 1 with a demand result.

[0035] In the WWW server 2, the authentication demand means 22 transmits the user information passed from the user demand means 21 to the authentication processing means 41 of an authentication server 4, and receives an authentication result from that of an authentication server 4.

[0036] When authentication is successful by the authentication server 4, the authentication demand means 22 of the WWW server 2 requires authentication information generation of the authentication information generation means 23. The authentication demand means 22 returns the authentication information generated with the authentication information generation means 23 to the user demand processing means 21.

[0037] In the WWW server 2, according to the demand from the authentication demand means 22, the authentication information generation means 23 generates authentication information, and returns the result. From the authentication demand means 22, user information is passed and this user information and a hour entry are included in authentication information.

[0038] The 2nd WWW server 3 is equipped with the user demand processing means 31 and the authentication cooperation processing means 34.

[0039] In the 2nd WWW server 3, the user demand processing means 31 processes the demand sent from the user demand transceiver means 11 like the user demand processing means 21. Delivery and its result are obtained for the authentication information transmitted with the demand for the authentication cooperation processing means 34. When authentication is successful, a demand result is transmitted to the user demand transceiver means 11.

[0040] In the 2nd WWW server 3, the authentication cooperation processing means 34 verifies rightness to the authentication information passed from the user demand processing means 31. From user information or a hour entry, the rightness of authentication information is checked and the result is returned to the user demand processing means 31.

[0041] An authentication server 4 is equipped with the authentication processing means 41 and the user management tool 42. The authentication processing means 41 receives user information from the authentication demand means 22. The information which the received user information is passed to the user management tool 42, and suits is looked for. When the information which suits with the user management tool 42 is found, as for the authentication processing means 41, the notice of an "authentication success" is returned to the authentication demand means 22 of the WWW server 2. On the other hand, when the information which suits with the user management tool 42 is not found, as for the authentication processing means 41, the notice of "authentication failure" is returned to the authentication demand means 22.

[0042] The user management tool 42 discovers the information which suits from the management information to hold to the user information passed from the authentication processing means 41, and delivers the result.

[0043] Drawing 2 is a flow chart for explaining actuation of one example of this invention. With reference to drawing 1 and drawing 2, actuation of the one whole example of this invention is explained to a detail.

[0044] A demand of a user is transmitted to the user demand processing means 21 of the WWW server 2 from the user demand transceiver means 11 of a terminal 1 (steps A1 and A2 of drawing 2). In this case, since user information is transmitted, the user demand processing means 21 takes out user information (step A3 of drawing 2).

[0045] When the user demand processing means 21 fails in the ejection of user information as a result of processing, it is judged as that to which user information is not correctly transmitted from the user demand transceiver means 11, and, as for the user demand processing means 21, an error is transmitted to the user demand transceiver means 11 (step A4 of drawing 2).

[0046] The user demand transceiver means 11 receives an error, and the result is shown on the screen of the display of a terminal 1 to a user (step A5 of drawing 2). In step A3 of drawing 2, the user information taken out correctly is passed to the authentication demand means 22, and authentication judging processing is further required of the authentication processing means 41 of an authentication server 4 (step A6 of drawing 2).

[0047] The authentication processing means 41 of an authentication server 4 receives user information (step A7 of drawing 2). Furthermore, in order that the authentication processing means 41 may investigate whether authentication is successful, it suits the user management tool 42 with delivery and the information managed in the target user information, or investigates (step A8 of drawing 2). This processing consists of inspection of User ID and a password currently conducted by computer. As a result of processing, when authentication goes wrong, the result is passed to the authentication demand means 22, and the user demand processing means 21 transmits an error to the user demand transceiver means 11 of a terminal 1 further (step A9 of drawing 2).

[0048] The user demand transceiver means 11 receives an error, and the result is shown in the screen superiors of a terminal 1 to a user (step A10 of drawing 2).

[0049] At step A8 of drawing 2, when an authentication judging is successful, the authentication demand means 22 requests generation of authentication information from the authentication information generation means 23 according to the result. In that case, user information is passed from the authentication demand means 22, and the authentication information generation means 23 generates a hour entry to the received user information and authentication information (step A11 of drawing 2).

[0050] The generated authentication information is received and passed to the user demand processing means 21 with the result of "an authentication success" from the authentication demand means 22. The user demand processing means 21 transmits a user's demand result and authentication information to the user demand transceiver means 11, and the result is shown on the screen of a terminal 1 to a user (steps A12

and A13 of drawing 2).

[0051] Then, in order to access the 2nd WWW server 3 with which a user cooperates, a demand is transmitted to the user demand processing means 31 from the user demand transceiver means 11 (step A14 of drawing 2). The user demand processing means 31 of the 2nd WWW server 3 receives this demand (step A15 of drawing 2), and takes out the authentication information automatically transmitted with this demand from the user demand transceiver means 11 (step A16 of drawing 2). When the user demand processing means 31 fails in the ejection of authentication information as a result of processing, the user demand processing means 31 is judged to be that to which authentication information is not correctly transmitted from the user demand transceiver means 11, and an error is transmitted to the user demand transceiver means 11 of a terminal 1 (step A17 of drawing 2). The user demand transceiver means 11 of a terminal 1 receives an error, and the result is shown on the screen of a terminal 1 to a user (step A18 of drawing 2).

[0052] In step A16 of drawing 2 , the authentication information correctly taken out with the user demand processing means 31 of the 2nd WWW server 3 is passed to the authentication cooperation processing means 34 from the user demand processing means 31 (step A19 of drawing 2).

[0053] The authentication cooperation processing means 34 of the 2nd WWW server 3 verifies rightness of authentication information from the user information included in the passed authentication information, or a hour entry (drawing 2 step A20).

Becoming authentication failure when verification is not successful, the user demand processing means 31 transmits an error to the user demand transceiver means 11 of a terminal 1 (step A21 of drawing 2).

[0054] The user demand transceiver means 11 receives an error, and the result is shown on a terminal 1 to a user (step A22 of drawing 2). In step A20 of drawing 2 , when an authentication judging is successful, the authentication cooperation processing means 34 returns the result of an authentication success to the user demand processing means 31. The user demand processing means 31 transmits a user's demand result to the user demand transceiver means 11 of a terminal 1, and the result is shown on a terminal 1 to a user (steps A23 and A24 of drawing 2).

[0055] Next, the authentication information generated in step A11 of drawing 2 is explained. Drawing 3 is drawing for explaining an example of the authentication information generated. As shown in drawing 3 , authentication information consists of user information or a hour entry. User information is included in the information transmitted in step A1 of drawing 2 . A hour entry is current time (present time information; for example, a date, which a system clock shows, time stump of time of day (at the time a part, a second)) which the WWW server 2 and the WWW server 3 of drawing 1 hold as a system. The check data generated from the information with which user information and a hour entry were combined are added to authentication information, and encryption processing is performed further.

[0056] Authentication cooperation judging processing of step A20 of drawing 2 is explained. Drawing 4 is a flow chart for explaining authentication cooperation judging processing.

[0057] Reference of drawing 4 performs a decryption at step B1 of drawing 4 to the enciphered authentication information which shows authentication cooperation judging processing to drawing 3.

[0058] Inspection of check data is conducted to the authentication information to which the decryption was carried out (step B-2 of drawing 4).

[0059] As a result of step B-2 of drawing 4, when check data are abnormalities, authentication cooperation is failing (step B5 of drawing 4).

[0060] When check data are normal, user information and a hour entry are taken out (step B3 of drawing 4), and inspection of whether a hour entry is in the time amount set to the authentication cooperation processing means 34 of drawing 1 is conducted (step B4 of drawing 4).

[0061] When this inspection goes wrong, authentication cooperation is judged to be failure (step B5 of drawing 4), and when inspection is successful, it is judged as an authentication cooperation success (step B6 of drawing 4).

[0062] The processing and a function are realized by the program by which each means of the user demand processing means 21 of the WWW server 2 explained in the above-mentioned example, the authentication demand means 22 and the authentication information generation means 23, the user demand processing means 31 of the WWW server 3, and the authentication cooperation processing means 34 is performed by computer of the WWW servers 2 and 3.

[0063] Next, other examples of this invention are explained to a detail with reference to a drawing. Drawing 5 is drawing showing the configuration of the 2nd example of this invention. In addition to the configuration of the WWW server 2 of said example which the WWW server 5 showed to drawing 1, this example is equipped with the authentication cooperation processing means 54 if drawing 5 is referred to. Moreover, in addition to the configuration of the 2nd WWW server 3 of said example shown in drawing 1, the WWW server 6 is equipped with the authentication demand means 62 and the authentication information generation means 63. That is, each WWW server is equipped with the user demand processing means, the authentication demand means, the authentication information generation means, and the authentication cooperation processing means.

[0064] As opposed to the authentication information passed by the authentication cooperation means 54 of the WWW server 5 from the user demand means 21 as well as the authentication cooperation means 34 in said example Rightness is verified, when the rightness of authentication information is checked and authentication is successful from user information or a hour entry further, new authentication information is required from the authentication information generation means 23, and the generated authentication information is returned to the user demand processing

means 21.

[0065] The authentication demand means 62 of the WWW server 6 transmits the user information passed from the user demand means 31 to the authentication processing means 41, and receives an authentication result. When authentication is successful, authentication information generation is required from the authentication information generation means 63, and the generated authentication information is returned to the user demand processing means 31.

[0066] According to the demand from the authentication demand means 62, the authentication information generation means 63 of the WWW server 6 generates authentication information, and returns the result.

[0067] From the authentication demand means 62 of the WWW server 6, user information is passed and the user information and hour entry are included in authentication information.

[0068] Drawing 6 is a flow chart for explaining actuation of the 2nd example of this invention. Actuation of the user demand transceiver means 11 in the 2nd example of this invention shown by step A1–A22 of drawing 6, the user demand processing means 21, the authentication demand means 22, the authentication information generation means 23, the authentication processing means 41, and the user management tool 42 Since it is the same as that of actuation (step A1–A22 of drawing 2) of each means 11, 21, 22, 23, 41, and 42 of the example shown in drawing 1, the explanation is omitted.

[0069] In said example, the authentication cooperation processing means 34 checked only the rightness of authentication information, and had returned the result to the user demand processing means 31.

[0070] In this example, when an authentication judging is successful at step A20 of drawing 6, the authentication cooperation processing means 34 of the WWW server 6 requests generation of authentication information from the authentication information generation means 63.

[0071] With the authentication cooperation processing means 34, the user information acquired from authentication information is passed to the authentication information generation means 63 of the WWW server 6, and authentication information is generated from the user information and hour entry (step C1 of drawing 6). The generated authentication information is received and passed to the user demand processing means 31 with the result of an authentication success from the authentication cooperation processing means 34.

[0072] The user demand processing means 31 of the WWW server 6 transmits a user's demand result and authentication information to the user demand transceiver means 11, and the result is shown on a terminal 1 to a user (steps A23 and A24 of drawing 6).

[0073] Thus, the authentication information generated by the authentication cooperation processing means 63 of the WWW server 6 can perform further

authentication cooperation processing by the user demand transceiver means 11 of a terminal 1 being passed.

[0074] Next, actuation of the further authentication cooperation processing is explained with reference to drawing 5 and drawing 7. In drawing 5, in order that a user may access the WWW server 5 from a terminal 1, the demand is transmitted to the user demand processing means 21 of the WWW server 5 from the user demand transceiver means 11 (step D1 of drawing 7).

[0075] The user demand processing means 21 of the WWW server 5 receives the demand (step D2 of drawing 7), and takes out user information (step D3 of drawing 7). When the user demand processing means 21 succeeds in the ejection of user information as a result of processing, it shifts to the authentication cooperation processing using user information (step D4 of drawing 7). Since the authentication cooperation processing using user information is the same as the processing after step A6 of drawing 2, explanation is omitted.

[0076] When the user demand processing means 21 fails in the ejection of user information at step D3 of drawing 7, the authentication information automatically transmitted with the demand is taken out from the user demand transceiver means 11 (step D5 of drawing 7).

[0077] When the user demand processing means 21 fails in the ejection of authentication information as a result of processing, it judges that authentication information is not correctly transmitted from the user demand transceiver means 11, and, as for the user demand processing means 21, an error is transmitted to the user demand transceiver means 11 (step D6 of drawing 7).

[0078] The user demand transceiver means 11 of a terminal 1 receives an error, and the result is shown on a terminal 1 to a user (step D7 of drawing 7).

[0079] In step D5 of drawing 7, the authentication information taken out correctly is passed to the authentication cooperation processing means 54 from the user demand processing means 21 (step D8 of drawing 2). The authentication cooperation processing means 54 verifies rightness of authentication information from the user information included in the passed authentication information, or a hour entry (drawing 7 step D9).

[0080] When verification is not successful, it becomes authentication failure and the user demand processing means 21 transmits an error to the user demand transceiver means 11 (step D10 of drawing 7).

[0081] The user demand transceiver means 11 receives an error, and the result is shown on a terminal 1 to a user (step D11 of drawing 7).

[0082] When an authentication judging is successful at step D9 of drawing 7, the authentication cooperation processing means 54 requests generation of authentication information from the authentication information generation means 23.

[0083] With the authentication cooperation processing means 54, the user information acquired from authentication information is passed to the authentication information

generation means 23, and authentication information is generated from the user information and hour entry (step D12 of drawing 7).

[0084] The generated authentication information is received and passed to the user demand processing means 21 with the result of an authentication success from the authentication cooperation processing means 54.

[0085] The user demand processing means 21 transmits a user's demand result and authentication information to the user demand transceiver means 11, and the result is shown on a terminal 1 to a user (steps D13 and D14 of drawing 2).

[0086] In the system configuration shown in drawing 5 following on step D13 of drawing 7, when a user accesses the WWW server 6 further, this can process authentication cooperation by the same processing as step A14 of drawing 2 or subsequent ones. In the system configuration shown in drawing 5, when a user accesses the WWW server 5 further from a terminal 1, this can process authentication cooperation by the same processing as step D1 of drawing 7 or subsequent ones.

[0087] Moreover, in the system configuration shown in drawing 5, if the WWW server 5 and the WWW server 6 are replaced in each processing of drawing 6 even when a user accesses the WWW server 6 at first, it can process in the same actuation.

[0088] Since all WWW servers have an authentication cooperation processing means and an authentication information generation means, this 2nd example has the new effectiveness that authentication cooperation can be processed by all WWW servers, even when the demand from a user continues two or more times. Furthermore, since user authentication processing to which an authentication processing server uses an authentication server only for access of the beginning from a user to a WWW server in the distributed environment which consists of the WWW server of the same configuration of that it can use in common is performed and authentication cooperation processing is performed in continuing access, it decreases and the count of access to an authentication processing server has the new effectiveness that the response air time to a demand of a user can be shortened.

[0089]

[Effect of the Invention] As explained above, when carrying out user authentication cooperation between information offer servers (WWW server) according to this invention, also in the environment where no information offer servers can use an authentication processing server, the effectiveness of being that user authentication is possible is done so.

[0090] The reason is because it considered as the configuration with which the justification is checked in this invention, without the authentication information generated after being attested by user information by the authentication server accessing an authentication server with the authentication cooperation processing means of the information offer server which cannot use an authentication processing server.

DESCRIPTION OF DRAWINGS

[Brief Description of the Drawings]

[Drawing 1] It is drawing showing the system configuration of one example of this invention.

[Drawing 2] It is a flow chart (flow chart) for explaining actuation of one example of this invention.

[Drawing 3] It is drawing for explaining creation of the authentication information in one example of this invention.

[Drawing 4] It is a flow chart (flow chart) for explaining actuation of the authentication cooperation processing in one example of this invention.

[Drawing 5] It is drawing showing the system configuration of other examples of this invention.

[Drawing 6] It is a flow chart (flow chart) for explaining actuation of other examples of this invention.

[Drawing 7] It is a flow chart (flow chart) for explaining actuation of authentication cooperation processing of other examples of this invention.

[Description of Notations]

- 1 Terminal
 - 2, 3, 5, 6 WWW server
 - 4 Authentication Server
 - 11 User Demand Transceiver Means
 - 21 User Demand Processing Means
 - 22 Authentication Demand Means
 - 23 63 Authentication information generation means
 - 31 User Demand Processing Means
 - 34 54 Authentication cooperation processing means
 - 41 Authentication Processing Means
 - 42 User Information Management Means
-

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号
特開2002-358283
(P2002-358283A)

(43) 公開日 平成14年12月13日 (2002. 12. 13)

(51) Int.Cl. ⁷	識別記号	F I	テ-マコード* (参考)
G 0 6 F 15/00	3 3 0	G 0 6 F 15/00	3 3 0 B 5 B 0 8 5
H 0 4 L 9/32		H 0 4 L 9/00	6 7 5 D 5 J 1 0 4

審査請求 有 請求項の数26 O L (全 16 頁)

(21) 出願番号 特願2001-166114(P2001-166114)

(22) 出願日 平成13年6月1日(2001. 6. 1)

(71) 出願人 000004237

日本電気株式会社
東京都港区芝五丁目7番1号

(72) 発明者 田中 広幸

東京都港区芝五丁目7番1号 日本電気株式会社内

(74) 代理人 100080816

弁理士 加藤 朝道

Fターム(参考) 5B085 AC12 AE02 AE23 BG07

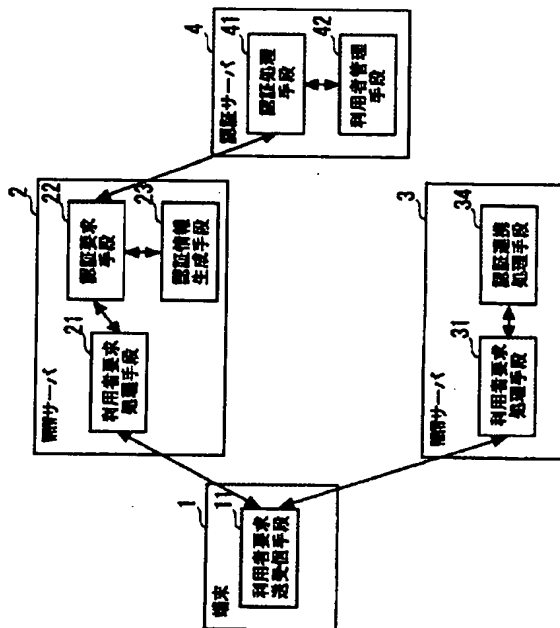
5J104 AA07 MA04 PA07

(54) 【発明の名称】 利用者認証連携方法及びシステム及びプログラム

(57) 【要約】

【課題】 認証を行うサーバを利用できないWWWサーバでも、認証の連携を可能とする利用者認証連携システム及び方法の提供。

【解決手段】 WWWサーバ2は、端末1が、利用者からの要求と、利用者認証を行うための利用者情報を受信し、前記利用者情報を認証サーバ4に送信する手段21、22と、認証サーバ4での認証が成功した場合に、前記利用者からの前記利用者情報と時間情報から認証情報の生成する認証情報生成手段23と、前記生成された認証情報を、要求結果と共に、前記端末に送信する手段21と、を備え、端末1は、WWWサーバ3に要求を送信する場合、認証情報を送信し、WWWサーバ3は認証情報から、利用者情報と時間情報を取り出し、認証の連携処理を行う認証連携処理手段34と、認証情報の正しさが検証され、前記利用者が認証された場合は、前記利用者の要求を受け付け、要求結果と共に、新たに生成した認証情報を、前記端末に送信する手段31とを備える。



【特許請求の範囲】

【請求項1】 端末からネットワークを介してアクセスされる一の情報提供サーバが、前記端末から送信された利用者情報を受け取り、前記利用者情報と時間情報とから認証情報を生成するステップと、
前記一の情報提供サーバが、生成した前記認証情報を、前記端末に送信するステップと、
前記端末からネットワークを介してアクセスされる情報提供サーバであって、認証の連携処理を行う情報提供サーバが、前記端末から送信された前記認証情報を受け取り、前記認証情報から、利用者情報と時間情報を取り出して、認証判定を行うステップと、
を含む、ことを特徴とする利用者認証連携方法。

【請求項2】 前記一の情報提供サーバは、前記端末から前記一の情報提供サーバに送信された前記利用者情報を、前記一の情報提供サーバに接続する認証サーバに送信するステップを実行し、前記認証サーバで認証が正しく行われた場合に、前記認証サーバでの認証結果を受けた前記一の情報提供サーバにおいて、前記認証情報を生成するステップと、前記認証情報を前記端末に送信するステップと、が実行される、ことを特徴とする請求項1記載の利用者認証連携方法。

【請求項3】 前記認証判定を行うステップで、認証が成功した場合、認証の連携処理を行う前記情報提供サーバでは、前記認証情報から前記利用者情報を取り出し、前記利用者情報と時間情報とから、あらたに認証情報を生成し、前記端末に、あらたに生成された前記認証情報を送信するステップを含む、ことを特徴とする請求項1記載の利用者認証連携方法。

【請求項4】 あらたに生成された前記認証情報を受信した前記端末が、認証の連携処理を行う情報提供サーバに要求を送信する場合に、前記認証情報を、認証の連携処理を行う前記情報提供サーバに送信するステップと、
認証の連携処理を行う前記情報提供サーバでは、前記端末から送信された前記認証情報を受け取り、前記認証情報から利用者情報と時間情報を取り出して、認証判定を行い、認証が成功した場合、前記認証情報から取り出された前記利用者情報と、時間情報から、あらたに認証情報を生成し、前記端末に、あらたに生成された前記認証情報を送信するステップと、
を含む、ことを特徴とする請求項3記載の利用者認証連携方法。

【請求項5】 前記認証情報の生成に用いられる前記時間情報が、前記認証情報を生成する情報提供サーバのシステム時計の時間情報である、ことを特徴とする請求項1乃至4のいずれかーに記載の利用者認証連携方法。

【請求項6】 端末が、利用者からの要求と、利用者認証を行うための利用者情報を、一の情報提供サーバに送信するステップと、
前記一の情報提供サーバでは、前記利用者情報を、前記

一の情報提供サーバが接続する認証サーバに送信し、前記認証サーバでの認証が成功した場合に、前記一の情報提供サーバの認証情報生成部にて、認証情報を生成するステップと、

前記一の情報提供サーバは、前記一の情報提供サーバの前記認証情報生成部で生成された前記認証情報を、要求結果と共に、前記端末に送信するステップと、

前記端末が、前記一の情報提供サーバと連携し、認証の連携処理を行う他の情報提供サーバに要求を送信する場合、前記要求とともに、前記認証情報を、前記他の情報提供サーバを送信するステップと、

前記他の情報提供サーバでは、前記端末から送信された前記認証情報を受け取り、認証連携処理部で、受け取った前記認証情報を基に、認証の連携処理を行うステップと、

前記他の情報提供サーバにおいて、前記認証の連携処理によって、認証情報の正しさが検証され、前記利用者が認証された場合には、前記利用者の要求を受け付け、要求結果と共に、新たに生成した認証情報を、前記端末に送信するステップと、

を有する、ことを特徴とする利用者認証連携方法。

【請求項7】 前記認証情報生成部で生成される認証情報が、利用者情報と時間情報と、チェックデータとを含み、これらの情報が暗号化されている、ことを特徴とする請求項6記載の利用者認証連携方法。

【請求項8】 前記認証連携処理部で認証の連携処理を行うステップが、

受け取った前記認証情報を復号するステップと、
復号された前記認証情報のチェックデータを検査するステップと、

前記チェックデータの検査が成功した場合、復号された前記認証情報から利用者情報と時間情報を取り出すステップと、

前記取り出された時間情報に基づき時間の検査を行うステップと、

前記時間検査が成功した場合、認証成功とするステップと、

を含む、ことを特徴とする請求項6又は7記載の利用者認証連携方法。

【請求項9】 利用者からの要求に対し、最初の情報提供サーバへのアクセスの場合、前記認証サーバを利用した利用者認証処理を行い、

続く情報提供サーバへのアクセスでは情報提供サーバでの認証連携処理を行う、ことを特徴とする請求項6又は7記載の利用者認証連携方法。

【請求項10】 前記一の情報提供サーバが認証の認証連携を行う認証連携処理部を有し、

前記一の情報提供サーバでは、前記端末から送信された認証情報を受け取り、前記認証連携処理部で認証の連携処理を行い、認証判定が成功した場合、前記一の情報提

供サーバの認証情報生成部に認証情報の生成を依頼するステップと、

前記一の情報提供サーバの前記認証情報生成部は、前記一の情報提供サーバの前記認証連携処理部が前記認証情報から取得した利用者情報を受け取り、前記利用者情報と時間情報とから認証情報を生成するステップと、を含む、ことを特徴とする請求項6記載の利用者認証連携方法。

【請求項11】認証の連携処理を行う前記他の情報提供サーバが認証情報生成部を有し、

前記他の情報提供サーバの認証連携処理部で認証の連携処理を行い、認証判定が成功した場合、前記他の情報提供サーバの認証情報生成部に認証情報の生成を依頼するステップと、

前記他の情報提供サーバの認証情報生成部は、前記認証連携処理部が前記認証情報から取得した利用者情報を受け取り、前記利用者情報と時間情報とから認証情報を生成するステップと、

前記他の情報提供サーバが、利用者の要求結果と、生成した前記認証情報を前記端末に送信するステップと、を含む、ことを特徴とする請求項6又は10記載の利用者認証連携方法。

【請求項12】端末からネットワークを介してアクセスされる一の情報提供サーバが、

前記端末から入力され前記一の情報提供サーバに送信された利用者情報と、前記一の情報提供サーバでの時間情報とから認証情報を生成し、生成した前記認証情報を、前記端末に送信する手段を備え、

前記端末からネットワークを介してアクセスされる情報提供サーバであって、認証の連携処理を行う情報提供サーバが、前記端末から送信された前記認証情報を受け取り、前記認証情報を復号して利用者情報及び時間情報を取り出し、認証判定を行う手段を備えている、ことを特徴とする利用者認証連携システム。

【請求項13】端末と、該端末からネットワークを介してアクセスされる複数の情報提供サーバと、を有し、前記複数の情報提供サーバには、認証サーバに接続される少なくとも一つの情報提供サーバと、認証の連携処理を行う少なくとも一つの情報提供サーバと、が含まれ、前記認証サーバに接続される一の情報提供サーバは、前記端末が、利用者からの要求と、利用者認証を行うための利用者情報を、前記一の情報提供サーバに送信した場合、これを受信し、前記利用者情報を、前記認証サーバに送信する手段と、

前記認証サーバでの認証が成功した場合に、前記利用者情報と時間情報から認証情報を生成する認証情報生成手段と、

前記生成された認証情報を、要求結果と共に、前記端末に送信する手段と、を備え、

前記端末は、認証の連携処理を行う前記情報提供サーバに要求を送信する場合、前記一の情報提供サーバより送信された前記認証情報を、認証の連携処理を行う前記情報提供サーバに送信する手段を備え、

認証の連携処理を行う前記情報提供サーバは、前記認証情報から、利用者情報と時間情報を取り出し、認証の連携処理を行う認証連携処理手段と、

前記認証の連携処理によって、認証情報の正しさが検証され、前記利用者が認証された場合は、前記利用者の要求を受け付け、要求結果と共に、新たに生成した認証情報を、前記端末に送信する手段とを備えている、ことを特徴とする利用者認証連携システム。

【請求項14】前記一の情報提供サーバの前記認証情報生成手段が、前記利用者情報と、時間情報と、チェックデータとからなる情報を暗号化したものを、前記認証情報として出力する、ことを特徴とする請求項13記載の利用者認証連携システム。

【請求項15】利用者からの要求に対し、最初の情報提供サーバへのアクセスの場合、前記認証サーバを利用した利用者認証処理を行い、続くアクセスでは、情報提供サーバの認証連携処理を行うことを特徴とする請求項13記載の利用者認証連携システム。

【請求項16】前記一の情報提供サーバが、前記端末からの利用者の要求を処理する利用者要求処理手段と、

前記認証サーバに対して認証要求を行い、前記認証サーバで認証が成功した場合、認証情報を生成するように要求する認証要求手段と、

を備え、

前記認証情報生成手段は、前記認証要求手段からの要求を受けて、前記利用者情報と時間情報とから前記認証情報を生成し、

前記利用者要求処理手段は、前記端末に対して、要求結果と、前記生成された認証情報とを送信する、ことを特徴とする請求項13記載の利用者認証連携システム。

【請求項17】認証の連携処理を行う前記情報提供サーバが、

前記端末からの利用者の要求を処理する利用者要求処理手段を備え、

前記認証連携処理手段が、前記端末から要求とともに送信される認証情報を受け取り、前記認証情報を基に、認証の連携処理を行い、

前記認証連携処理手段での認証連携処理によって、認証情報の正しさが検証され、前記利用者が認証された場合には、前記利用者要求処理手段では、前記利用者の要求を受け付け、要求結果と共に、新たに生成された前記認証情報を、前記端末に送信する、ことを特徴とする請求項13記載の利用者認証連携システム。

【請求項18】前記認証連携処理手段が、前記認証情報を復号する手段と、

復号された前記認証情報のチェックデータを検査する手段と、
前記チェックデータの検査結果が正しい場合、復号された前記認証情報から利用者情報と時間情報を取り出す手段と、
前記時間情報の検査を行う手段と、
を含み、前記時間情報の検査結果が正しい場合、認証成功とする、ことを特徴とする請求項13記載の利用者認証連携システム。

【請求項19】前記一の情報提供サーバが、認証連携処理手段をさらに備え、
前記一の情報提供サーバは、前記端末から送信された認証情報を受け取り、前記一の情報提供サーバの前記認証連携処理手段で認証連携を行い、認証判定が成功した場合、前記一の情報提供サーバの前記認証情報生成手段に対して認証情報の生成を依頼し、
前記一の情報提供サーバの前記認証情報生成手段は、前記認証連携処理手段が前記認証情報から取得した利用者情報を受け取り、前記利用者情報と時間情報から認証情報を生成する、ことを特徴とする請求項13記載の利用者認証連携システム。

【請求項20】認証の連携処理を行う前記情報提供サーバが、認証情報生成手段を備え、
認証の連携処理を行う前記情報提供サーバが、前記認証連携処理手段で認証連携を行い、認証判定が成功した場合、認証の連携処理を行う前記情報提供サーバの前記認証情報生成手段に認証情報の生成を依頼し、
認証の連携処理を行う前記情報提供サーバの前記認証情報生成手段が、前記認証連携処理手段が前記認証情報から取得した利用者情報を受け取り、利用者情報と時間情報とから認証情報を生成し、利用者の要求結果と前記認証情報を前記端末に送信する、ことを特徴とする請求項13又は19記載の利用者認証連携システム。

【請求項21】端末からネットワークを介してアクセスされる一の情報提供サーバが、

(a) 前記端末から利用者からの要求と、利用者認証を行うための利用者情報を受信し、前記利用者情報を、前記認証サーバに送信する処理と、

(b) 前記認証サーバでの認証が成功した場合に、前記利用者情報と時間情報から認証情報を生成する認証情報生成処理と、

(c) 前記生成された認証情報を、要求結果と共に、前記端末に送信する処理と、
を有し、
端末からネットワークを介してアクセスされ前記一の情報提供サーバと認証の連携処理を行う情報提供サーバが、

(d) 前記端末から送信された前記認証情報から、利用者情報と時間情報を取り出し、認証の連携処理を行う認証連携処理と、

(e) 前記認証連携処理によって、認証情報の正しさが検証され、前記利用者が認証された場合は、前記利用者の要求を受け付け、要求結果と共に、新たに生成した認証情報を、前記端末に送信する処理とを含み、
前記各処理を前記各情報提供サーバで実行させるためのプログラム。

【請求項22】請求項21記載のプログラムにおいて、
前記認証情報生成処理で、前記利用者情報と時間情報とチェックデータとから、認証情報を生成し、さらにこの認証情報を暗号化する処理を、
前記情報提供サーバで実行させるためのプログラム。

【請求項23】請求項21記載のプログラムにおいて、
前記認証連携処理が、
前記認証情報を復号する処理と、
復号された前記認証情報のチェックデータを検査する処理と、
前記チェックデータの検査結果が正しい場合、復号された前記認証情報から利用者情報と時間情報を取り出す処理と、
前記時間情報の検査を行う処理と、
を含み、
前記各処理を、前記情報提供サーバで実行させるためのプログラム。

【請求項24】端末からネットワークを介してアクセスされる情報提供サーバが、
前記端末より送信される、利用者認証を行うための利用者情報を受信し、前記利用者情報を、前記認証サーバに送信する手段と、
前記認証サーバでの認証が成功した場合に、前記利用者情報と時間情報から認証情報を生成する認証情報生成手段と、
前記生成された認証情報を前記端末に送信する手段と、
を備えている、ことを特徴とする情報提供サーバ装置。

【請求項25】端末とネットワーク接続され前記端末より送信される利用者情報を受信し、前記利用者情報と時間情報から認証情報を生成し、前記生成した認証情報を前記端末に送信する手段を備えた情報提供サーバ装置と、
認証の連携処理を行う情報提供サーバであって、
前記端末から送信された前記認証情報から、利用者情報と時間情報を取り出し、認証の連携処理を行う認証連携処理手段と、

前記認証の連携処理によって、認証情報の正しさが検証され、前記利用者が認証された場合は、前記利用者の要求を受け付け、要求結果と共に、新たに生成した認証情報を、前記端末に送信する手段とを備えている、ことを特徴とする情報提供サーバ装置。

【請求項26】前記認証連携処理手段が、
前記認証情報を復号する手段と、
復号された前記認証情報のチェックデータを検査する手段と、

前記チェックデータの検査結果が正しい場合、復号された前記認証情報から利用者情報と時間情報を取り出す手段と、

前記時間情報の検査を行う手段と、

を含み、前記時間情報の検査結果が正しい場合、認証成功とする、ことを特徴とする請求項24記載の情報提供サーバ装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、認証システム及び方法に関し、特にサーバで認証連携処理を行う方法とシステムと装置並びにプログラムに関する。

【0002】

【従来の技術】利用者認証連携システムとして、例えば特開平11-31129号公報には、複数のWWW(World Wide Web)サーバを備えたネットワークシステムにおいて、利用者は一度認証すれば、認証有効時間内は、付与された一意の不可視のIDをもとに、複数ページや異なるWWWサーバにわたってアクセスを可能としたWWWサーバ連携システムが提案されている。このWWWサーバ連携システムにおいて、セッションIDを用いて連携を処理するホストは、複数のいずれかのWWWサーバから通知されたブラウザからHTML(HyperText Markup Language)文書を解析し、セッションIDが付与されていなかったときに、ユーザ情報の入力要求を、WWWサーバを介してブラウザに送信し、送信されたユーザ情報を解析して登録の許可された要求に対して一意のセッションIDを生成し、再び、WWWサーバを介してセッションIDを埋め込んだHTML文書をブラウザに送信するとともに、有効時間情報を管理し、有効時間情報範囲内のとき、認証を許可する。すなわち、認証が必要な場合、端末によって送信されたID、パスワードはWWWサーバを経由してホストに送信され、認証が行われる。ホストによって認証が成功した場合、ホストによりセッションIDが生成され、そのセッションIDは、結果と共にWWWサーバ経由で端末に送られ、利用者からのアクセス時には、端末から送信される要求には、セッションIDが自動的に付加されており、そのセッションIDはホストによって検証される。

【0003】しかしながら、この利用者認証連携システムは、次のような問題点を有している。

【0004】第1の問題点は、ホストが利用できないWWWサーバとは連携ができない、ということである。その理由は、セッションIDの検証、生成が、専ら、ホストで行われる、ためである。

【0005】第2の問題点は、利用者からの要求が増大した場合、そのレスポンスが低下する、ということである。その理由は、すべてのWWWサーバは、すべての利用者からのアクセスごとに、同一のホストに対して、セッションIDの検証や生成を要求する構成とされてい

る、ためである。

【0006】また特開2000-222360号公報には、クライアント手段と、認証サーバ手段と、認可サーバ手段を備え、クライアント手段は、認証サーバと、秘密情報を共有し、認証サーバ手段は、秘密情報を不可逆演算 f を n 回行った照合情報を含む認証チケットを発行し、クライアント手段は認可サーバに、不可逆演算 f を $n-k$ 回行った提示情報を示し、認可サーバは、提示情報に不可逆演算 f を k 回行って照合情報と一致するかチェックする認証システム、方法が提案されている。このシステムも、認証サーバ手段と、認可サーバ手段に接続できない、WWWサーバ、端末では、適用できない。また、例えば特開平10-177552号公報には、クライアントと複数のサーバ間に認証応答管理部を有する代理サーバを設け、認証応答管理部が、クライアントを認証し、一旦認証したクライアントについて複数のサーバに対する認証情報の応答を代行する認証応答方法と装置が開示されている。

【0007】

【発明が解決しようとする課題】したがって本発明が解決しようとする課題は、認証を行うサーバを利用できないWWWサーバでも、認証の連携を可能とする方法及びシステムと装置並びにプログラムを提供することにある。

【0008】

【課題を解決するための手段】前記課題を解決するための手段を提供する本発明に係る方法は、端末からネットワークを介してアクセスされる一の情報提供サーバが、前記端末から入力され前記一の情報提供サーバに送信された利用者情報と、前記一の情報提供サーバでの時間情報とから、認証情報を生成し、生成した前記認証情報を、前記端末に送信するステップと、前記端末からネットワークを介してアクセスされる情報提供サーバであって、認証の連携処理を行う情報提供サーバでは、前記端末から送信された前記認証情報を受け取り、前記認証情報を復号して利用者情報及び時間情報を取り出し、認証判定を行うステップと、を含む。

【0009】本発明に係る方法は、端末が、利用者からの要求と、利用者認証を行うための利用者情報を、一の情報提供サーバに送信するステップと、前記一の情報提供サーバでは、前記利用者情報を、認証サーバに送信し、前記認証サーバでの認証が成功した場合に、前記一の情報提供サーバの認証情報生成部にて、認証情報を生成するステップと、前記一の情報提供サーバは、前記一の情報提供サーバの前記認証情報生成部で生成された前記認証情報を、要求結果と共に、前記端末に送信するステップと、前記端末が、前記一の情報提供サーバと連携し、認証の連携処理を行う他の情報提供サーバに要求を送信する場合、前記認証情報を、前記他の情報提供サーバを送信するステップと、前記他の情報提供サーバで

は、前記端末から送信された前記認証情報を受け取り、認証連携処理部で、前記認証情報を基に、認証の連携処理を行うステップと、前記他の情報提供サーバにおいて、前記認証の連携処理によって、認証情報の正しさが検証され、前記利用者が認証された場合には、前記利用者の要求を受け付け、要求結果と共に、新たに生成した認証情報を、前記端末に送信するステップと、を有する。

【0010】別のアスペクトにおいて、本発明に係るシステムは、端末からネットワークを介してアクセスされる一の情報提供サーバが、前記端末から入力され前記一の情報提供サーバに送信された利用者情報と、前記一の情報提供サーバでの時間情報とから、認証情報を生成し、生成した前記認証情報を、前記端末に送信する手段を備え、前記端末からネットワークを介してアクセスされる情報提供サーバであって、認証の連携処理を行う情報提供サーバが、前記端末から送信された前記認証情報を受け取り、前記認証情報を復号して利用者情報及び時間情報を取り出し、認証判定を行う手段を備えている。

【0011】さらに、別のアスペクトにおいて、本発明に係るプログラムは、端末からネットワークを介してアクセスされる一の情報提供サーバが、(a) 前記端末から利用者からの要求と、利用者認証を行うための利用者情報を受信し、前記利用者情報を、前記認証サーバに送信する処理と、(b) 前記認証サーバでの認証が成功した場合に、前記利用者情報と時間情報から認証情報を生成する認証情報生成処理と、(c) 前記生成された認証情報を、要求結果と共に、前記端末に送信する処理と、を有し、端末からネットワークを介してアクセスされ前記一の情報提供サーバと認証の連携処理を行う情報提供サーバが、(d) 前記端末から送信された前記認証情報から、利用者情報と時間情報を取り出し、認証の連携処理を行う認証連携処理と、(e) 前記認証連携処理によって、認証情報の正しさが検証され、前記利用者が認証された場合は、前記利用者の要求を受け付け、要求結果と共に、新たに生成した認証情報を、前記端末に送信する処理とを含み、前記各処理を前記各情報提供サーバで実行させるためのプログラムよりなる。

【0012】

【発明の実施の形態】本発明の実施の形態について説明する。本発明は、その好ましい一実施の形態において、ブラウザ機能を有する端末(図1の1)から、IP(Internet Protocol)網等のネットワークを介してアクセスされる情報提供サーバ(WWW(World Wide Web)サーバ)(図1の2)が、端末(図1の1)から入力されWWWサーバ(2)に送信された利用者情報を受け取る手段(図1の21)と、利用者情報と、前記一のWWWサーバでの時間情報とから、認証情報を生成する手段(図1の23)と、生成した前記認証情報を、前記端末に送信する手段(図1の21)を備えている。また端末(図

1の1)からネットワークを介してアクセスされ、認証の連携処理を行うWWWサーバ(図1の3)は、端末(図1の1)から送信された認証情報を受け取る手段(図1の31)と、該認証情報を復号して利用者情報及び時間情報を取り出し、時間検査を行うことで認証判定を行う手段(図1の34)を備えている。

【0013】本発明は、その好ましい一実施の形態において、認証サーバ(図1の4)に接続される一のWWWサーバ(図1の2)は、端末(図1の1)が、利用者からの要求と、利用者認証を行うための利用者情報を、WWWサーバ(図1の2)に送信した場合、これを受信し、前記利用者情報を認証サーバ(図1の4)に送信する手段(図1の21、22)と、認証サーバ(図1の4)での認証が成功した場合に、前記利用者の前記利用者情報と時間情報から認証情報を生成する認証情報生成手段(図1の23)と、前記生成された認証情報を、要求結果と共に、前記端末に送信する手段(図1の21)と、を備えている。

【0014】端末(図1の1)は、認証の連携処理を行うWWWサーバ(図1の3)に要求を送信する場合、WWWサーバ(図1の2)より送信された前記認証情報を、認証の連携処理を行う前記WWWサーバ(図1の3)に送信する手段(図1の11)を備えている。

【0015】認証の連携処理を行うWWWサーバ(図1の3)は、前記認証情報から、利用者情報と時間情報を取り出し、認証の連携処理を行う認証連携処理手段(図1の34)と、前記認証の連携処理によって、認証情報の正しさが検証され、前記利用者が認証された場合は、前記利用者の要求を受け付け、要求結果と共に、新たに生成した認証情報を、前記端末に送信する手段(図1の31)とを備えている。

【0016】本発明は、その好ましい一実施の形態において、前記一のWWWサーバで生成される認証情報が、利用者情報と時間情報と、チェックデータとを含み、これらの情報が暗号化されている。

【0017】認証の連携処理を行うWWWサーバ(図1の3)において、認証連携処理手段(図1の34)は、認証情報を復号する手段(図4のB1)と、復号された認証情報のチェックデータを検査する手段(図4のB2)と、該チェックデータの検査結果が正しい場合、復号された認証情報から利用者情報と時間情報を取り出す手段(図4のB3)と、前記時間情報の検査を行う手段(図4のB4)と、を含み、前記時間情報の検査結果が正しい場合、認証成功とする。

【0018】本発明の別の実施の形態において、上記した認証情報生成手段(図5の23)を備えたWWWサーバ(図5の5)が、認証連携処理手段(図5の54)をさらに備えた構成としてもよい。WWWサーバ(図5の5)は、端末(図5の1)から送信された認証情報を受け取り、認証連携処理手段(図5の54)で認証連携を行

い、認証判定が成功した場合、認証情報生成手段（図5の54）に対して認証情報の生成を依頼し、認証情報生成手段（図5の23）は、認証連携処理手段（図5の54）が前記認証情報から取得した利用者情報を受け取り、利用者情報と時間情報から認証情報を生成する。

【0019】認証の連携処理を行うWWWサーバ（図5の6）が、認証情報生成手段（図5の63）をさらに備えた構成としてもよい。認証の連携処理を行う前記WWWサーバ（図5の6）が、前記認証連携処理手段（図5の34）で認証連携を行い、認証判定が成功した場合、認証の連携処理を行うWWWサーバ（図5の6）の前記認証情報生成手段（図5の63）に認証情報の生成を依頼し、前記認証情報生成手段（図5の63）が、前記認証連携処理手段（図5の34）が前記認証情報から取得した利用者情報を受け取り、利用者情報と時間情報とから認証情報を生成し、利用者の要求結果と認証情報を前記端末に送信する。

【0020】WWWサーバにおける認証情報生成手段、認証連携処理手段は、WWWサーバのノードコンピュータで実行されるプログラムによりその処理、機能が実現される。

【0021】複数のWWWサーバが、利用者を認証する場合に、認証処理サーバが共通的に利用できない環境である場合には、WWWサーバが認証処理サーバを利用することなしに、利用者の認証の連携をできるようにしている。

【0022】図1は、本発明の一実施の形態のシステム構成を示す図である。図1において、端末（1）は、WWWサーバ（2）等にインターネットプロトコル網等のネットワークを介して接続され、端末（1）から入力された認証用の利用者情報は、WWWサーバ（2）を介して認証サーバ（4）に提供される。

【0023】端末（1）の利用者要求送受信手段（11）は、利用者からの要求を、WWWサーバ（2）の利用者要求処理手段（21）に送信する。送信される要求には、初回時には利用者認証を行うための利用者ID、パスワードなどのような利用者情報が共に送信される。

【0024】WWWサーバ（2）の利用者要求処理手段（21）は、利用者情報を認証要求手段（22）に送信する。認証要求手段（22）は、認証サーバ（4）の認証処理手段（41）にその利用者情報を送信し、その利用者が利用可能かの結果を待つ。

【0025】認証サーバ（4）の認証処理手段（41）で認証が成功した場合、認証成功という結果がWWWサーバ（2）の認証要求手段（22）に返され、認証要求手段（22）は、認証情報生成手段（23）に、認証情報の生成を依頼する。

【0026】WWWサーバ（2）の利用者要求処理手段（21）は、認証情報生成手段（23）によって生成された認証情報を、その要求結果と共に、端末（1）の利

用者要求送受信手段（11）に送信する。この認証情報には、利用者情報や時間情報が含まれ、利用者が続く要求を送信する場合、利用者要求送受信手段（11）が自動的に共に送信するようになっている。

【0027】続いて利用者が、WWWサーバ（2）と連携する第2のWWWサーバ（3）の利用者要求処理手段（31）に要求を送信した場合、共に、認証情報が送信される。

【0028】その場合、その認証情報を基に、WWWサーバ（3）の認証連携処理手段（34）で認証連携処理が行われる。

【0029】認証連携処理によって、認証情報の正しさが検証され、利用者が認証された場合は、その利用者の要求を受け付けることになるが、WWWサーバ（3）の利用者要求処理手段（31）は、その要求結果を、端末（1）の利用者要求送受信手段（11）に送信する。

【0030】これにより、認証処理サーバを利用することなしに、利用者連携を行うことを可能にする。

【0031】

【実施例】上記した実施の形態についてさらに具体的かつ詳細に説明すべく本発明の実施例について説明する。図1は、本発明の一実施例のシステム構成の一例を示す図である。図1を参照すると、本発明の一実施例に係るシステムは、利用者が要求を送受信する端末1と、その利用者要求を処理するWWWサーバ2と、WWWサーバ2と連携してその利用者要求を処理する第2のWWWサーバ3と、利用者の認証情報を処理する認証サーバ4とを含む。なお、この実施例において、WWWサーバが提供する情報の内容、種類は問わないが、処理要求の実行にあたり、利用者の認証が必要とされるものとする。

【0032】端末1は、利用者の要求をWWWサーバに送信し、WWWサーバからの処理結果を受信する利用者要求送受信手段11を備える。利用者要求送受信手段11は、要求を送信する際には、WWWサーバ2の認証情報生成手段23が生成した認証情報がある場合には、該要求と共に自動的に送信する。要求が処理された場合には、WWWサーバ2の利用者要求処理手段21や、WWWサーバ3の利用者要求処理手段31から送信される要求結果を受信する。

【0033】WWWサーバ2は、利用者要求処理手段21と、認証要求手段22と、認証情報生成手段23とを備える。

【0034】WWWサーバ2において、利用者要求処理手段21は、利用者要求送受信手段11から送られてきた要求を処理する。初回要求時には、要求と共に送信されてきた利用者ID、パスワードのような利用者情報を認証要求手段22に渡し、認証結果を得る。認証サーバ2での認証が成功し、WWWサーバ2が要求結果を、端末1に送信する際には、認証情報生成手段23にて生成された認証情報を、要求結果と共に、端末1の利用者要

求送受信手段11に送信する。

【0035】WWWサーバ2において、認証要求手段22は、利用者要求手段21から渡された利用者情報を、認証サーバ4の認証処理手段41に送信し、認証サーバ4のから認証結果を受け取る。

【0036】認証サーバ4で認証が成功した場合には、WWWサーバ2の認証要求手段22は、認証情報生成手段23に、認証情報生成を要求する。認証要求手段22は、認証情報生成手段23で生成された認証情報を、利用者要求処理手段21に返す。

【0037】WWWサーバ2において、認証情報生成手段23は、認証要求手段22からの要求に従い、認証情報を生成し、その結果を返す。認証要求手段22からは利用者情報が渡され、認証情報には、該利用者情報や時間情報が含まれる。

【0038】第2のWWWサーバ3は、利用者要求処理手段31と、認証連携処理手段34を備える。

【0039】第2のWWWサーバ3において、利用者要求処理手段31は、利用者要求処理手段21と同様、利用者要求送受信手段11から送られてきた要求を処理する。要求と共に送信されてきた認証情報を認証連携処理手段34に渡し、その結果を得る。認証が成功した場合は、要求結果を利用者要求送受信手段11に送信する。

【0040】第2のWWWサーバ3において、認証連携処理手段34は、利用者要求処理手段31から渡された認証情報に対し、正しさの検証を行う。利用者情報や時間情報から、認証情報の正しさが確認され、その結果を利用者要求処理手段31に返す。

【0041】認証サーバ4は、認証処理手段41と、利用者管理手段42とを備える。認証処理手段41は、認証要求手段22から利用者情報を受け取る。受け取った利用者情報は、利用者管理手段42に渡され適合する情報が探される。もし、利用者管理手段42で適合する情報が見つかった場合には、認証処理手段41は、「認証成功」の通知を、WWWサーバ2の認証要求手段22に返す。一方、利用者管理手段42で適合する情報が見つからなかった場合には、認証処理手段41は、「認証失敗」の通知を認証要求手段22に返す。

【0042】利用者管理手段42は、認証処理手段41から渡された利用者情報に対し、保持する管理情報から適合する情報を探し出し、その結果を受け渡す。

【0043】図2は、本発明の一実施例の動作を説明するためのフローチャートである。図1及び図2を参照して、本発明の一実施例の全体の動作について詳細に説明する。

【0044】端末1の利用者要求送受信手段11から利用者の要求が、WWWサーバ2の利用者要求処理手段21に送信される(図2のステップA1およびA2)。この場合、利用者情報が送信されるので、利用者要求処理手段21は、利用者情報を取り出す(図2のステップA

3)。

【0045】処理の結果、利用者要求処理手段21が利用者情報の取り出しに失敗した場合、利用者情報が利用者要求送受信手段11から正しく送信されてきてないものと判断し、利用者要求処理手段21は、エラーを、利用者要求送受信手段11に送信する(図2のステップA4)。

【0046】利用者要求送受信手段11は、エラーを受信し、その結果は、利用者に対して、端末1の表示装置の画面上に示される(図2のステップA5)。図2のステップA3において、正しく取り出された利用者情報は、認証要求手段22に渡され、さらに、認証サーバ4の認証処理手段41に、認証判定処理が要求される(図2のステップA6)。

【0047】認証サーバ4の認証処理手段41は、利用者情報を受信する(図2のステップA7)。さらに認証処理手段41は、認証が成功するか調べるため、対象となる利用者情報を利用者管理手段42に渡し、管理されている情報と適合するか調査を行う(図2のステップA8)。この処理は、例えば、コンピュータで行われている、利用者IDとパスワードの検査からなる。処理の結果として、認証が失敗した場合は、その結果が認証要求手段22に渡され、さらには利用者要求処理手段21が、エラーを、端末1の利用者要求送受信手段11に送信する(図2のステップA9)。

【0048】利用者要求送受信手段11は、エラーを受信し、その結果は、利用者に対し端末1の画面上等に表示される(図2のステップA10)。

【0049】図2のステップA8にて、認証判定が成功した場合、認証要求手段22は、その結果に従い、認証情報生成手段23に認証情報の生成を依頼する。その際、認証要求手段22から利用者情報が渡され、認証情報生成手段23は、受け取った利用者情報や、時間情報から、認証情報を生成する(図2のステップA11)。

【0050】生成された認証情報は、認証要求手段22から利用者要求処理手段21に「認証成功」という結果と共に受け渡される。利用者要求処理手段21は、利用者の要求結果と認証情報を、利用者要求送受信手段11に送信し、その結果は、利用者に対して端末1の画面上に示される(図2のステップA12、およびA13)。

【0051】引き続き、利用者が連携する第2のWWWサーバ3にアクセスするため、利用者要求送受信手段11から、利用者要求処理手段31に要求が送信される(図2のステップA14)。第2のWWWサーバ3の利用者要求処理手段31は該要求を受信し(図2のステップA15)、利用者要求送受信手段11から該要求と共に自動的に送信された認証情報を取り出す(図2のステップA16)。処理の結果、利用者要求処理手段31が認証情報の取り出しに失敗した場合、利用者要求処理手段31は、認証情報が利用者要求送受信手段11から正

しく送信されてきてないものと判断し、エラーを、端末1の利用者要求送受信手段11に送信する(図2のステップA17)。端末1の利用者要求送受信手段11は、エラーを受信し、その結果は、利用者に対し端末1の画面上に示される(図2のステップA18)。

【0052】図2のステップA16において、第2のWWWサーバ3の利用者要求処理手段31で正しく取り出された認証情報は、利用者要求処理手段31から、認証連携処理手段34に渡される(図2のステップA19)。

【0053】第2のWWWサーバ3の認証連携処理手段34は、渡された認証情報に含まれる利用者情報や時間情報から、認証情報の正しさの検証を行う(図2ステップA20)。検証が成功しなかった場合は認証失敗となり、利用者要求処理手段31は、エラーを端末1の利用者要求送受信手段11に送信する(図2のステップA21)。

【0054】利用者要求送受信手段11は、エラーを受信し、その結果は利用者に対し端末1上に示される(図2のステップA22)。図2のステップA20において、認証判定が成功した場合、認証連携処理手段34は、利用者要求処理手段31に認証成功という結果を返す。利用者要求処理手段31は、利用者の要求結果を、端末1の利用者要求送受信手段11に送信し、その結果は利用者に対し端末1上に示される(図2のステップA23、およびA24)。

【0055】次に、図2のステップA11において生成される認証情報について説明する。図3は、生成される認証情報の一例を説明するための図である。図3に示すように、認証情報は、利用者情報や時間情報から成る。利用者情報は、図2のステップA1において送信される情報に含まれているものである。時間情報は、図1のWWWサーバ2やWWWサーバ3がシステムとして保持する現在時刻(システムクロックの示す現在の時刻情報;例えば年月日、時刻(時、分、秒)のタイムスタンプ)である。認証情報には、利用者情報や時間情報が組み合わされた情報から生成されるチェックデータが付加され、さらに、暗号化処理が施される。

【0056】図2のステップA20の認証連携判定処理について説明する。図4は、認証連携判定処理を説明するためのフローチャートである。

【0057】図4を参照すると、認証連携判定処理は、図3に示す暗号化された認証情報に対して、図4のステップB1にて、復号化が行われる。

【0058】復号化が行われた認証情報に対して、チェックデータの検証が行われる(図4のステップB2)。

【0059】図4のステップB2の結果として、チェックデータが異常の場合は、認証連携は失敗となる(図4のステップB5)。

【0060】チェックデータが正常の場合、利用者情報

と時間情報が取り出され(図4のステップB3)、時間情報が、図1の認証連携処理手段34に定められている時間内であるか否かの検査が行われる(図4のステップB4)。

【0061】この検査が失敗した場合には、認証連携は失敗と判断され(図4のステップB5)、検査が成功した場合には、認証連携成功と判断される(図4のステップB6)。

【0062】上記実施例で説明したWWWサーバ2の利用者要求処理手段21、認証要求手段22、及び認証情報生成手段23、WWWサーバ3の利用者要求処理手段31、認証連携処理手段34の各手段は、WWWサーバ2、3のコンピュータで実行されるプログラムによりその処理、機能が実現される。

【0063】次に、本発明の他の実施例について図面を参照して詳細に説明する。図5は、本発明の第2の実施例の構成を示す図である。図5を参照すると、本実施例は、WWWサーバ5が、図1に示した前記実施例のWWWサーバ2の構成に加え、認証連携処理手段54を備えている。またWWWサーバ6は、図1に示した前記実施例の第2のWWWサーバ3の構成に加え、認証要求手段62と認証情報生成手段63と、を備えている。すなわち、各WWWサーバは、利用者要求処理手段と、認証要求手段と、認証情報生成手段と、認証連携処理手段を備えている。

【0064】WWWサーバ5の認証連携手段54は、前記実施例における認証連携手段34と同様に、利用者要求手段21から渡された認証情報に対して、正しさの検証を行い、さらに、利用者情報や時間情報から、認証情報の正しさが確認され、認証が成功した場合には、認証情報生成手段23に対して新しい認証情報を要求し、生成されたその認証情報を、利用者要求処理手段21に返す。

【0065】WWWサーバ6の認証要求手段62は、利用者要求手段31から渡された利用者情報を、認証処理手段41に送信し、認証結果を受け取る。認証が成功した場合には、認証情報生成手段63に対して認証情報生成を要求し、生成されたその認証情報を利用者要求処理手段31に返す。

【0066】WWWサーバ6の認証情報生成手段63は、認証要求手段62からの要求に従い、認証情報を生成し、その結果を返す。

【0067】WWWサーバ6の認証要求手段62からは、利用者情報が渡され、認証情報にはその利用者情報や時間情報が含まれる。

【0068】図6は、本発明の第2の実施例の動作を説明するためのフローチャートである。図6のステップA1-A22で示される、本発明の第2の実施例における利用者要求送受信手段11、利用者要求処理手段21、認証要求手段22、認証情報生成手段23、認証処理手

段41および利用者管理手段42の動作は、図1に示された実施例の各手段11、21、22、23、41および42の動作（図2のステップA1-A22）と同一であるため、その説明は、省略する。

【0069】前記実施例では、認証連携処理手段34は、単に、認証情報の正しさのみを確認し、その結果を利用者要求処理手段31に返していた。

【0070】この実施例では、図6のステップA20にて、認証判定が成功した場合、WWWサーバ6の認証連携処理手段34は、認証情報生成手段63に、認証情報の生成を依頼する。

【0071】WWWサーバ6の認証情報生成手段63には、認証連携処理手段34によって認証情報から得られた利用者情報が渡され、その利用者情報や時間情報から認証情報が生成される（図6のステップC1）。生成された認証情報は、認証連携処理手段34から利用者要求処理手段31に認証成功という結果と共に受け渡される。

【0072】WWWサーバ6の利用者要求処理手段31は、利用者の要求結果と認証情報を、利用者要求送受信手段11に送信し、その結果は利用者に対し端末1上に表示される（図6のステップA23、およびA24）。

【0073】このようにWWWサーバ6の認証連携処理手段63によって生成された認証情報が、端末1の利用者要求送受信手段11に渡されることで、さらなる認証連携処理を行うことができる。

【0074】次に、図5と図7を参照して、さらなる認証連携処理の動作について説明する。図5において、利用者が端末1からWWWサーバ5にアクセスするため、その要求が、利用者要求送受信手段11から、WWWサーバ5の利用者要求処理手段21に送信される（図7のステップD1）。

【0075】WWWサーバ5の利用者要求処理手段21はその要求を受信し（図7のステップD2）、利用者情報を取り出す（図7のステップD3）。処理の結果、利用者要求処理手段21が利用者情報の取り出しに成功した場合、利用者情報を用いた認証連携処理に移行する（図7のステップD4）。利用者情報を用いた認証連携処理は、図2のステップA6以降の処理と同一であるため、説明は省略する。

【0076】図7のステップD3にて、利用者要求処理手段21が利用者情報の取り出しに失敗した場合、利用者要求送受信手段11から要求と共に自動的に送信された認証情報を取り出す（図7のステップD5）。

【0077】処理の結果、利用者要求処理手段21が認証情報の取り出しに失敗した場合、認証情報が利用者要求送受信手段11から正しく送信されてきてないと判断し、利用者要求処理手段21はエラーを利用者要求送受信手段11に送信する（図7のステップD6）。

【0078】端末1の利用者要求送受信手段11はエラ

ーを受信し、その結果は利用者に対し端末1上に表示される（図7のステップD7）。

【0079】図7のステップD5において、正しく取り出された認証情報は、利用者要求処理手段21から認証連携処理手段54に渡される（図2のステップD8）。認証連携処理手段54は、渡された認証情報に含まれる利用者情報や時間情報から、認証情報の正しさの検証を行う（図7ステップD9）。

【0080】検証が成功しなかった場合は、認証失敗となり、利用者要求処理手段21がエラーを利用者要求送受信手段11に送信する（図7のステップD10）。

【0081】利用者要求送受信手段11は、エラーを受信し、その結果は、利用者に対し端末1上に表示される（図7のステップD11）。

【0082】図7のステップD9にて認証判定が成功した場合、認証連携処理手段54は、認証情報生成手段23に認証情報の生成を依頼する。

【0083】認証情報生成手段23には、認証連携処理手段54によって認証情報から得られた利用者情報が渡され、その利用者情報や時間情報から、認証情報が生成される（図7のステップD12）。

【0084】生成された認証情報は、認証連携処理手段54から利用者要求処理手段21に認証成功という結果と共に受け渡される。

【0085】利用者要求処理手段21は、利用者の要求結果と認証情報を、利用者要求送受信手段11に送信し、その結果は利用者に対し端末1上に表示される（図2のステップD13、およびD14）。

【0086】図7のステップD13に引き続き、図5に示すシステム構成において、利用者がさらにWWWサーバ6にアクセスをする場合、これは、図2のステップA14以降と同様の処理で認証連携を処理することができる。図5に示すシステム構成において、端末1から利用者がさらにWWWサーバ5にアクセスをする場合、これは、図7のステップD1以降と同様の処理で認証連携を処理することができる。

【0087】また、図5に示すシステム構成において、利用者がWWWサーバ6に最初アクセスをする場合でも、図6の各処理においてWWWサーバ5とWWWサーバ6を置き換えれば、同一の動作で処理を行うことができる。

【0088】この第2の実施例は、すべてのWWWサーバが、認証連携処理手段と認証情報生成手段を持つため、利用者からの要求が複数回続く場合でも、すべてのWWWサーバで認証連携を処理できるという新たな効果を有する。また、さらに認証処理サーバが共通的に利用できる同一構成のWWWサーバから成る分散環境において、利用者からWWWサーバへの最初のアクセスのみに、認証サーバを利用する利用者認証処理が行われ、続くアクセスでは認証連携処理が行われるため、認証処理

サーバへのアクセス回数が少なくなり、利用者の要求へのレスポンス送信時間が短縮できるという新たな効果を有する。

【0089】

【発明の効果】以上説明したように、本発明によれば、情報提供サーバ（WWWサーバ）間で利用者認証連携をする場合に、すべての情報提供サーバが認証処理サーバを利用できない環境においても、利用者認証ができることである、という効果を奏する。

【0090】その理由は、本発明においては、認証サーバで利用者情報により認証された後に生成される認証情報が、認証処理サーバを利用できない情報提供サーバの認証連携処理手段によって、認証サーバにアクセスすることなしに、その正当性が確認される、構成としたためである。

【図面の簡単な説明】

【図1】本発明の一実施例のシステム構成を示す図である。

【図2】本発明の一実施例の動作を説明するための流れ図（フローチャート）である。

【図3】本発明の一実施例における認証情報の作成を説

明するための図である。

【図4】本発明の一実施例における認証連携処理の動作を説明するための流れ図（フローチャート）である。

【図5】本発明の他の実施例のシステム構成を示す図である。

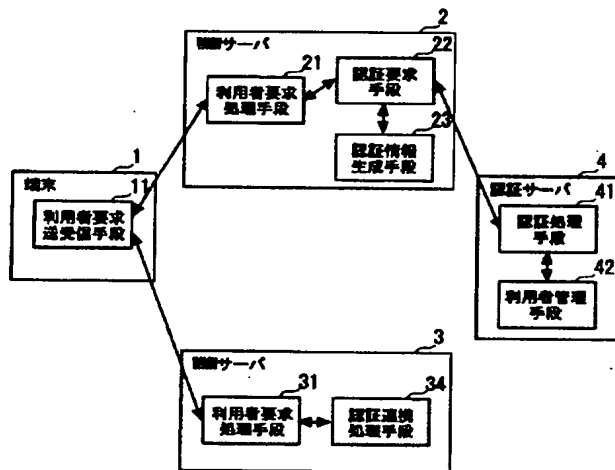
【図6】本発明の他の実施例の動作を説明するための流れ図（フローチャート）である。

【図7】本発明の他の実施例の認証連携処理の動作を説明するための流れ図（フローチャート）である。

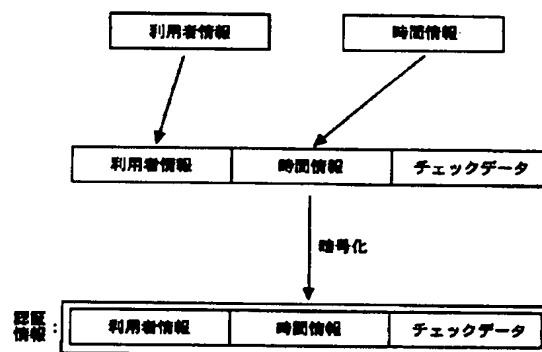
【符号の説明】

- 1 端末
- 2、3、5、6 WWWサーバ
- 4 認証サーバ
- 11 利用者要求送受信手段
- 21 利用者要求処理手段
- 22 認証要求手段
- 23、63 認証情報生成手段
- 31 利用者要求処理手段
- 34、54 認証連携処理手段
- 41 認証処理手段
- 42 利用者情報管理手段

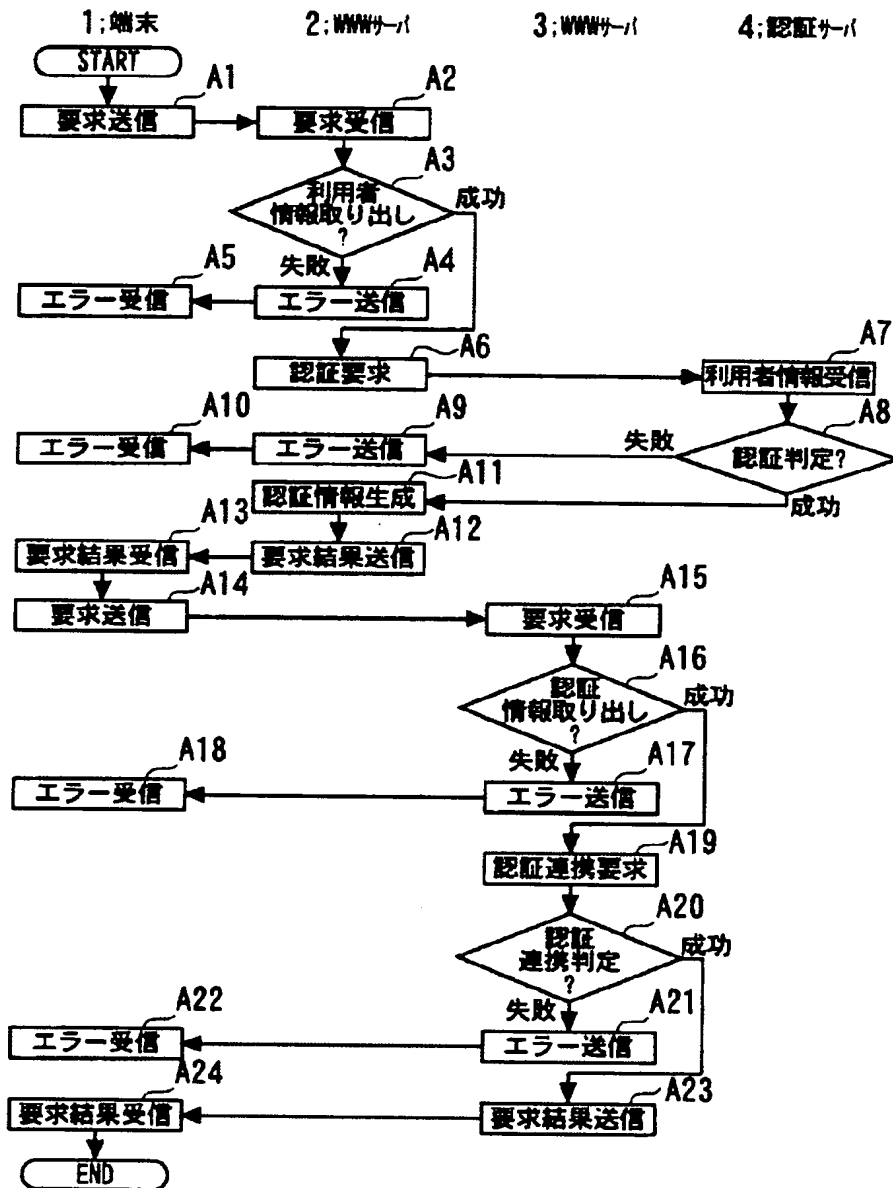
【図1】



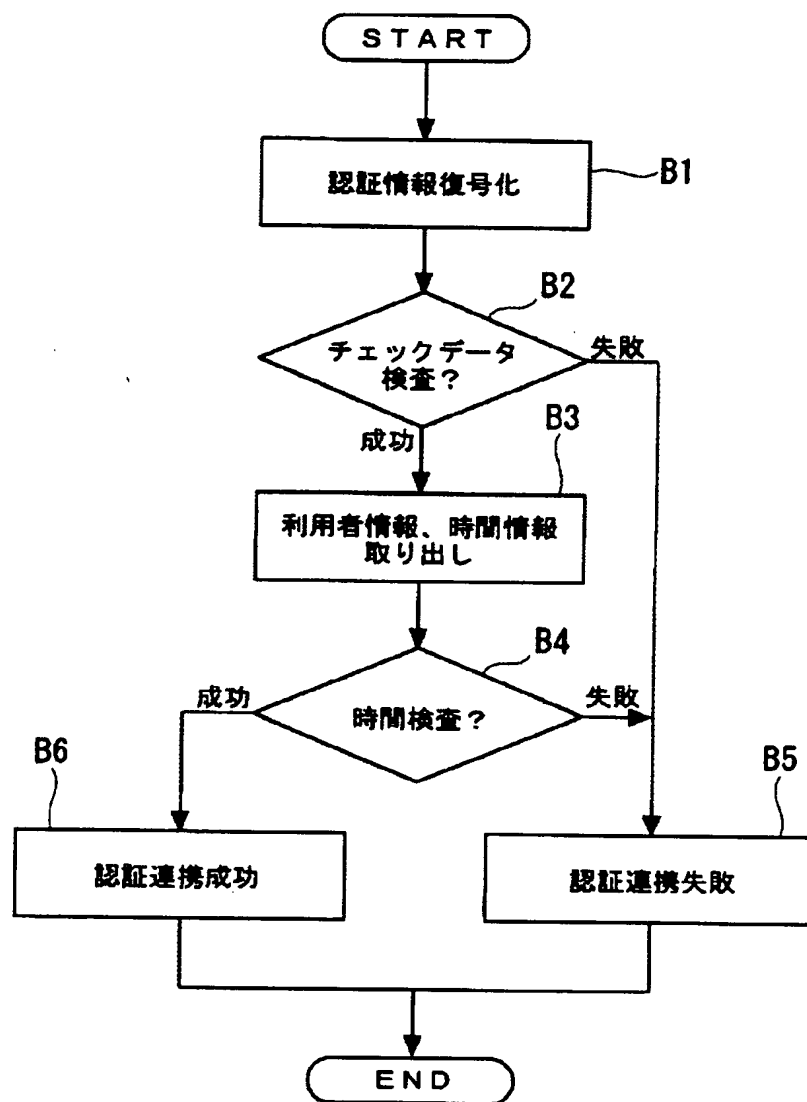
【図3】



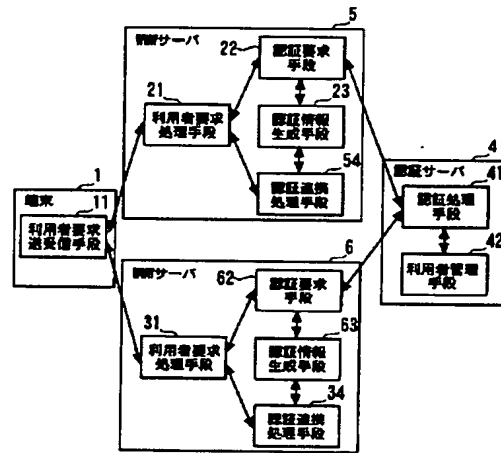
【図2】



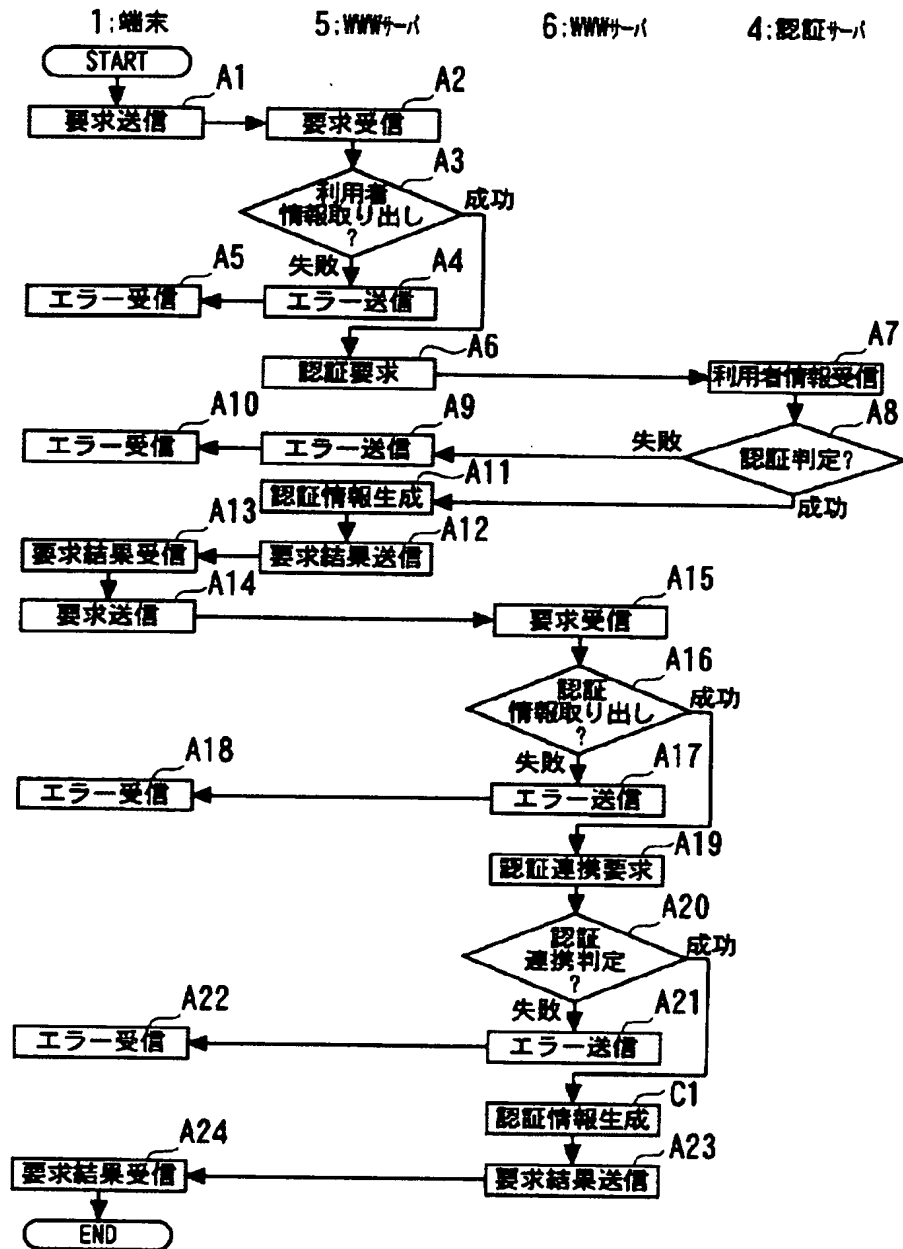
【図4】



【図5】



【図6】



【図7】

